

ESV 系列 VPN 防火墙使用说明书

深圳市鑫金浪电子有限公司
网址：www.kingnet.com.cn

声　　明

此商标 

为金浪网络的注册商标，不得仿冒。

前　　言

版本说明

本手册适用于金浪 ESV 系列 ESV-500,ESV-3200 企业级 VPN 防火墙。

内容介绍

这份手册主要介绍了金浪 ESV 系列 VPN 防火墙的硬件特性、常用功能的软件配置以及常见故障的排除等。

在安装 VPN 防火墙之前及安装过程中为避免可能出现的设备损坏和人身伤害，请仔细阅读本手册 。

建议:

建议由熟悉电气环境、线缆连接以及有实际安装和配置 VPN 防火墙经验的专业技术人进行安装和配置。

这份手册包括以下章节：

- **第一章 产品介绍**

介绍了金浪 ESV 系列 VPN 防火墙的外观图以及系统特性；

- **第二章 VPN 防火墙的安装**

介绍 VPN 防火墙的机械安装方法、电源连接方法、配置口电缆连接方法；

- **第三章 配置指南**

介绍如何启动并对 VPN 防火墙、搭建 VPN 防火墙的配置环境，且如何进行快速配置；

- **附录 A FAQ**

对用户的常用功能进行简单的实例解析说明。

读者对象

本书适合以下人员阅读：

- 网络工程师
- 技术推广人员
- 网络管理员

本书约定

1、通用格式约定

宋体：正文采用五号宋体。

警告、说明等提示等内容一律用楷体，并且在内容前后增加线条与正文隔离。

2、各类标志

本书还采用标记来表示应该注意的地方：

警告、危险、提醒操作中应注意的事项。 ：

说明、提示、窍门、对操作内容的描述进行必要的补充和说明。

目　　录

物　品　清　单

小心打开包装盒，检查包装盒里应有以下配件：
一台金浪ESV系列VPN防火墙
一条电源线
一张产品说明光盘
一张保修卡

注意
如果打开包装时发现产品有所损坏或者任何配件短缺的情况，请及时和当地经销商联系。

第一章 产品介绍

感谢您购买本公司的金浪ESV系列VPN防火墙。该系列产品是基于Intel Xscale技术的高性能VPN防火墙。

集专业VPN、防火墙与高性能宽带路由器于一体，提供强大VPN功能和防火墙功能的同时兼备企业宽带路由器的所有功能，将强大的功能集成到同一台设备中，既节省了企业的网络投资，更简化了企业的网络管理，为企业提供完整、安全、经济、高效的网络解决方案。

1.1 金浪 ESV- VPN 防火墙

1.1.1 金浪 ESV-500VPN 防火墙

金浪 ESV-500 是一款双 WAN 口 VPN 防火墙，具备 4 个百兆 LAN 口， VPN 防火墙提供强大的数据处理能力，同时为系统的稳定运行提供强力的硬件平台。

采用三层隧道协议 IPSec 协议。支持 50 条 IPSec 隧道数。可以轻松组建远程局域网，同时支持 MAC 地址及 IP 地址绑定，用户访问认证控制（ACL）；支持动态域名解析，支持无固定 IP 的应用，支持穿透 NAT 功能；内建先进防火墙功能，可防止 DoS 攻击、扫描、嗅探式攻击，有效防止 Nimda、冲击波、木马等病毒攻击，能灵活指定 IP、用户或应用分配最小/最大宽带和设定优先级，保证特殊用户、特殊应用（如 VoIP 等）的服务质量，还支持用户认证，方便制定安全策略的同时，有效防范上网权限盗用。提供中文 WEB 配置界面，配置直观方便。



产品型号	ESV-500
支持的标准和协议	IEEE802.3、IEEE802.3u、IEEE802.3x、TCP/IP、FTP、PPPoE、HTTP、TFTP、

		DHCP、NAT
端口	WAN	2 个 10/100M 自适应 RJ45 端口
	LAN	4 个 10/100M 自适应 RJ45 端口
网络介质		10Base-T:3 类或 3 类上 UTP 100Base-T：5 类 UTP
IPSec 隧道数		50
LED 指示	WAN	Link/Act(连接/工作)、100M
	LAN	Link/Act(连接/工作)、100M
	其它	Status（系统状态灯），Power（电源）
使用环境		工作温度：0ºC 到 40ºC；工作湿度：10%到 90%不凝结 存储温度：-40ºC 到 70ºC；存储湿度：5%到 90%不凝结
外形尺寸(LxWxH) 单位(mm)		440×205×43
输入电源 功耗		输入：220VAC，50Hz 功耗：最大 20W

1.1.2 金浪 ESV-3200VPN 防火墙

金浪 ESV-3200 是一款双 WAN 口 VPN 防火墙，具备 4 个百兆 LAN 口， VPN 防火墙提供强大的数据处理能力，同时为系统的稳定运行提供强力的硬件平台。

采用三层隧道协议 IPSec 协议。支持 200 条 IPSec 隧道数。可以轻松组建远程局域网，同时支持 MAC 地址及 IP 地址绑定，用户访问认证控制（ACL）；支持动态域名解析，支持无固定 IP 的应用，支持穿透 NAT 功能；内建先进防火墙功能，可防止 DoS 攻击、扫描、嗅探式攻击，有效防止 Nimda、冲击波、木马等病毒攻击，能灵活指定 IP、用户或应用分配最小/最大宽带和设定优先级，保证特殊用户、特殊应用（如 VoIP 等）的服务质量，还支持用户认证，方便制定安全策略的同时，有效防范上网权限盗用。提供中文 WEB 配置界面，配置直观方便。



产品型号	ESV-3200

支持的标准和协议		IEEE802.3、IEEE802.3u、IEEE802.3x、TCP/IP、FTP、PPPoE、HTTP、TFTP、DHCP、NAT
端口	WAN	2 个 10/100M 自适应 RJ45 端口
	LAN	4 个 10/100M 自适应 RJ45 端口
网络介质		10Base-T:3 类或 3 类上 UTP　100Base-T：5 类 UTP
IPSec 隧道数		200
LED 指示	WAN	Link/Act(连接/工作)、100M
	LAN	Link/Act(连接/工作)、100M
	其它	Status（系统状态灯），Power（电源）
使用环境		工作温度：0ºC 到 40ºC；工作湿度：10%到 90%不凝结 存储温度：-40ºC 到 70ºC；存储湿度：5%到 90%不凝结
外形尺寸(LxWxH) 单位(mm)		440×205×43
输入电源 功耗		输入：220VAC，50Hz 功耗：最大 20W

1.2 金浪 ESV -VPN 防火墙特点

1.2.1 建立可靠的 VPN 网络

采用三层隧道协议IPSec协议，分别支持50条/200条IPSec隧道数，可以轻松组建远程局域网。适合于一个企业和多个分支机构之间，来建立一个可靠，便捷，易维护和低成本的VPN 网络。使得企业各分支之间能够实时，安全的共享各种数据，运行以前只能在域局网上共享的各种业务软件。

1.2.2 兼并高性能路由器功能

允许多台计算机共享多条宽带连接和多个不同的 ISP 帐号同时连接因特网，几倍于普通路由器的带宽。可混合使用不同的因特网连接方式，如 Cable Modem，ADSL，ADSL PPPoE，LAN PPPoE 或 LAN to LAN 的高带宽网络连接，通过线路负载平衡设置将多条宽带连接达到最高效率的使用。

1.2.3 强大的防火墙功能—保障网络安全快捷

金浪 ESV 系列 VPN 防火墙是为用户提供高度网络安全和网络资源共享的极好产品。由于它包含强大的防火墙引擎， 所以能够防 DDOS/DOS 攻击，同时因为包含了数据包过滤，可以关闭

特殊端口，可以防止用户的私人网络免受因特网黑客袭击。

金浪 ESV 系列 VPN 防火墙除支持宽带路由器常见的功能外，还支持带宽控制、系统安全日志等高级功能，内建先进防火墙功能，数据包控制策略功能，可防止 DoS 攻击、扫描、嗅探式攻击，有效防止 Nimda、冲击波、木马等病毒攻击，能灵活指定 IP、用户或应用分配带宽和设定优先级，保证特殊用户、特殊应用（如 VoIP 等）的服务质量。

1.2.4 方便友好的用户管理界面—有助于网络维护

通过基于 WEB 页面的配置方式 ，金浪 ESV 系列 VPN 防火墙易于安装和维护。所有的功能均可通过浏览器来配置业务。本产品除了具有高效能的传输速率之外，更结合简易的设置接口，让用户在使用上本产品只需要极短的时间，便能完成基本的设置步骤，让用户使用起来更轻松更方便。

1.2.5 数据包控制策略管理—让内网管理变得更加轻松

通过 VPN 防火墙的数据包控制策略功能，能够实现对内网用户权限的管理。使得内网用户拥有不同的上网权限，也可以对内网用户进行上网限制，可支持 IP 限制，域名限制，应用软件(QQ 等)限制，实现企业网络管理严格化。

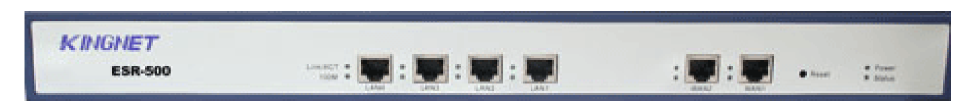
也可以通过内网 IP+MAC 地址绑定以及 IP 流量限制，对内网用户进行统一管理和带宽分配，充分体现了该 VPN 防火墙在路由器方面的作用，使得网络管理员更加轻松。

第二章　VPN 防火墙的安装

2.1 VPN 防火墙面板布置

2.1.1 前面板

此处以ESV-500的前面板为例：



LED 灯号说明

LED	描述	意义
Power	电源状态指示灯	绿灯常亮：　电源开启连接
Status	系统状态指示灯	绿灯常亮：VPN 防火墙非正常工作 绿灯闪烁：VPN 防火墙工作正常
Link/Act	端口连接/传输指示灯	绿灯常亮：以太网络联机正常 绿灯闪烁：以太网络端口正在传送/接收封包数据传输
100M	端口 100M 传输速率指示灯	绿灯常亮：以太网络端口传输速率为 100M
1000M	端口 1000M 传输速率指示灯	绿灯常亮：以太网络端口传输速率为 1000M

RESET键：

在WAN口和系统电源状态灯之间有一个小孔，为RESET键，此键可以用于恢复系统出厂值。

🕮 提示：如果您忘记了VPN防火墙的密码或**IP**地址，您可通过此按钮恢复出厂设置。VPN防火墙通电状态下，按住此按钮**10**秒以上，直到**Status**灯常亮后，松开按钮，即可恢复出厂设置。

2.1.2　后面板

VPN 防火墙后面板有一个电源接口。电源工作范围：180-260V～50Hz-60Hz。

➢ 电源插座

二线三相规格电源插座，把电源线阴性插头接到这个插座上，阳性插头接到交流电源上。

2.2 VPN 防火墙安装的注意事项

金浪ESV系列VPN防火墙承担着网络连接的中转站的重要作用，其正常使用关系到整个网络是否能正常运作.在VPN防火墙的安装和使用过程中特提出如下的安全建议:

- 请不要将VPN防火墙放置在有水的地方，也不要让液体进入VPN防火墙。
- 请将VPN防火墙放置在远离热源的地方。
- 请确认VPN防火墙的正常接地。
- 不要穿着松散的服装以防勾住器件造成损坏，为此请系紧衣带、围巾，扎好衣袖。
- 将工具、器件放在远离人员行走的地方以防碰。
- 建议用户使用 UPS 不间断电源，一方面可以避免断电，另一方面可以避免电源干扰。

金浪ESV系列VPN防火墙必须在室内使用，为保证VPN防火墙正常工作和延长使用寿命。安装场所应该满足下列要求：

- 温度/湿度要求
- 洁净度要求
- 防静电要求
- 抗干扰要求
- 防雷击要求
- 检查安装台

2.3 VPN 防火墙的连接

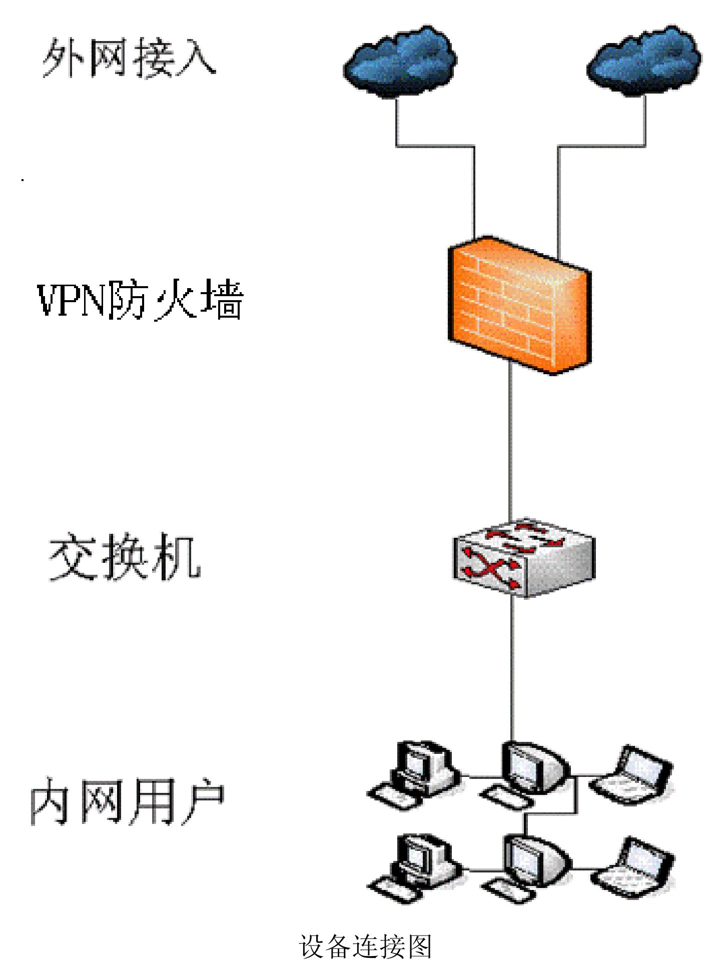
首先，请您参考以下步骤完成 VPN 防火墙的网络连接。

1) 建立局域网连接

用一根网线连接 VPN 防火墙的 LAN 口和局域网中的集线器或交换机。您也可以用一根网线将 VPN 防火墙 LAN 口与您的计算机网卡直接相连。

2)　建立广域网连接

广域网直接连接到 ADSL 或者光纤。



设备连接图

3)　连接电源

将电源连接好，VPN防火墙将自行启动。

第三章　　配置指南

这一章将给出金浪ESV系列VPN防火墙的功能配置说明。本章节的内容是根据金浪ESV系列VPN防火墙的配置界面项来进行列表，您可以更加直观的通过此说明对VPN防火墙进行配置。

3.1 WEB 管理的连接

3.1.1　准备工作

首先，必须确保管理电脑安装了网页浏览器软件(比如 Microsoft Internet Explorer，简称 IE)，而且浏览器必须支持 JavaScript 脚本功能。由于不同的浏览器对网页代码的解释不尽相同，为保证配置操作的准确无误，建议您使用微软的 Internet Explorer 浏览器，如果您使用 Netscape 浏览器，请确保其为最新版本。如果您使用 Internet Explorer 浏览器，请确保其版本在 5.0 以上，建议使用 6.0 版本。为了达到良好的浏览效果，建议您将显示分辨率设为 1024×768 或者更高。

如果您在配置本宽带 VPN 防火墙的时候，WEB 页面不能正常使用或者不能正常配置 VPN 防火墙，需要按照以下的说明来初始化操作系统的浏览器配置。一般情况下如果能够正确配置 VPN 防火墙的话，不需要更改浏览器的设　　置，此时请跳过以下几步。

为了使 WEB 方式的管理能正常进行，我们需要对所使用的网页浏览器软件进行配置，下面以 Windows XP 下 IE 6.0 为例说明 z。

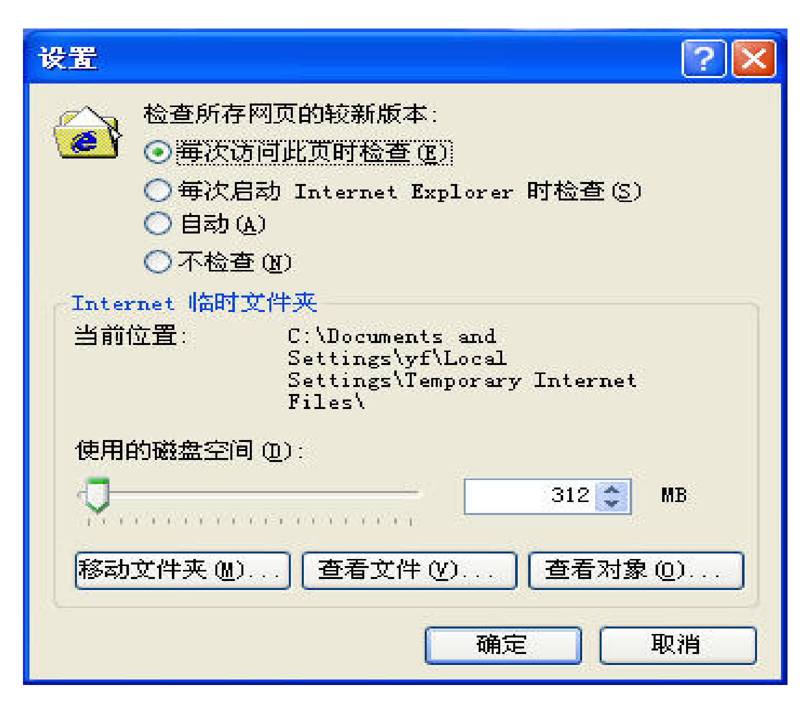
第一步在 IE 菜单中选择“工具”→“Internet 选项”，会弹出 Internet 选项对话框：



图：Internet 选项设置

第二步：点击“删除文件”，清除浏览器的缓存记录；特别需要时点击“删除 Cookies”清除自动登录记录（慎用）。

点击“设置”按钮，进入设置对话框，如下图所示：



图：设置对话框

如果您使用 Internet Explorer 5.0 版本的浏览器，请您务必选择“每次访问此页时检查”一项。否则将可能导致某些页面显示的 VPN 防火墙配置信息错误。

如果您使用 Internet Explorer 6.0 版本的浏览器，可以选择“每次访问此页时检查”项或“自动”项，建议选择后者。

选择完成后点击“确定”按钮即可。

注　意：

选择“每次访问此页时检查”项将使 Internet Explorer 浏览器在每次刷新时都会从 VPN 防火墙取完整的页面文件，而不是读取磁盘中的临时文件。这将保证配置信息的正确无误，但同时也可能导致页面的显示速度变慢。如果您选择了此项，在完成对 VPN 防火墙的 WEB 配置后，将其改为“自动”一项，否则您访问其它网页时显示速度将可能受到较大影响。Internet Explorer 6.0 对此问题处理较好，可以放心使用“自动”项(默认选项)。

第三步：请选择 Internet 选项对话框的“安全”标签，然后点击“自定义级别”按钮，如下图所示：



图：Internet 选项设置

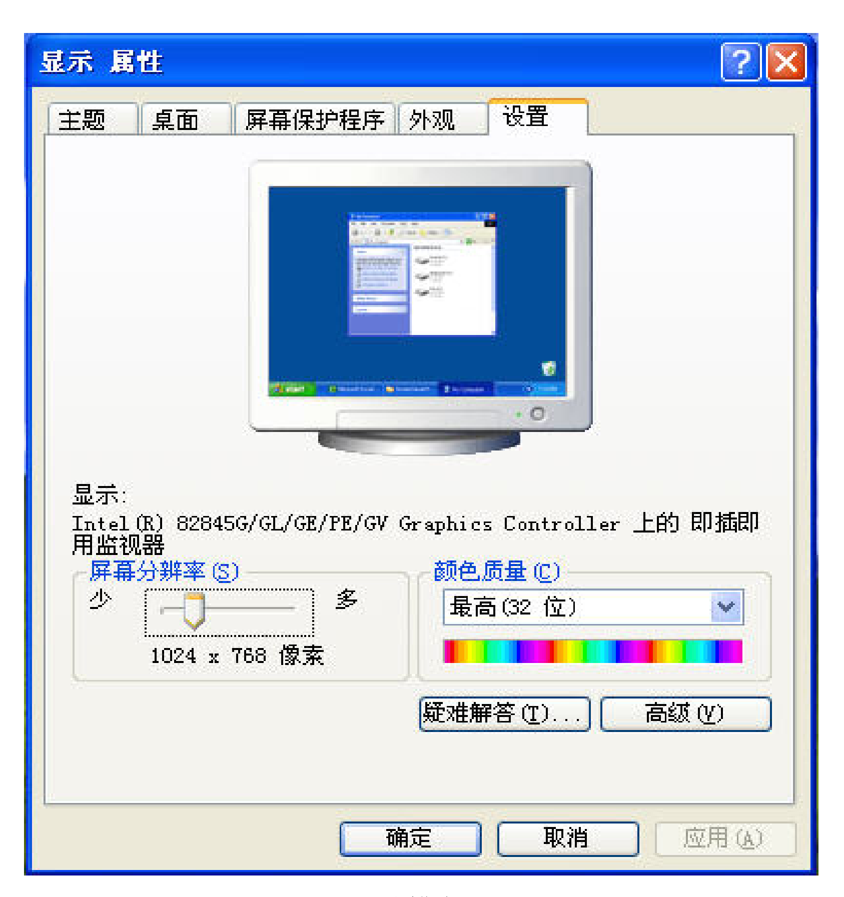
第四步如果上述操作正确无误，就会弹出以下的对话框：



图：安全设置

请选择活动脚本中的“启用”或者将“重置”下拉文本框设置成“安全级-中”，点击“重置”按钮，最后点击“确定”按钮。

第五步：在桌面上单击鼠标右键，选择弹出菜单中“属性”选项，将弹出显示属性对话框，如下图所示：



图：分辨率设置

请选择“设置”标签，将屏幕区域设置为 1024×768，并单击“应用”按钮。如果修改分辨率后感觉屏幕较为闪烁，请单击上图的“高级”按钮，在弹出窗口的“监视器”页面中调高显示刷新率，具体细节此处略过。

经过了以上设置，您就可以畅通无阻地通过 WEB 对 VPN 防火墙进行配置了。

注意:

将屏幕的分辨率设为 1024×768 是对 PC 硬件设备有一定要求的，对于硬件配置较低的 PC 可以不按此设置。

3.1.2 WEB 的连接

ESV系列VPN防火墙出厂时，默认登录地址为：https://192.168.0.254:10000。

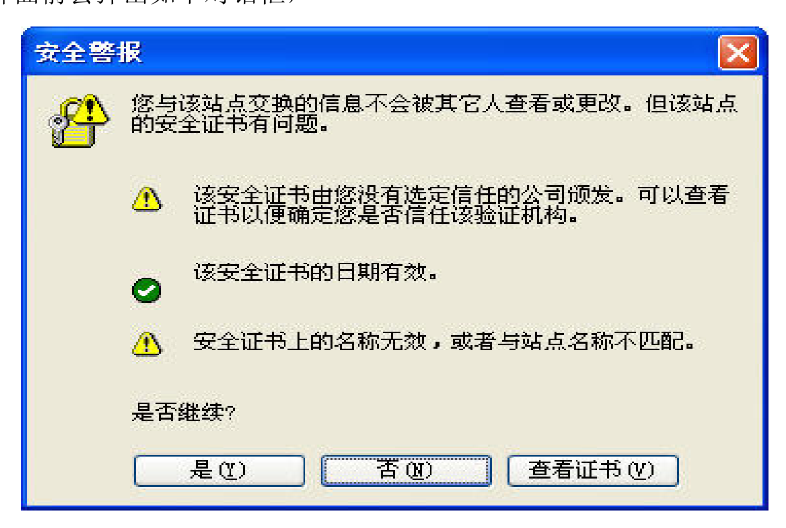
配置的默认用户名是 admin，口令是888888。

登录ESV系列VPN防火墙可对其进行配置时。如果您需要改变口令，也请参考后续相关章节的配置指导。

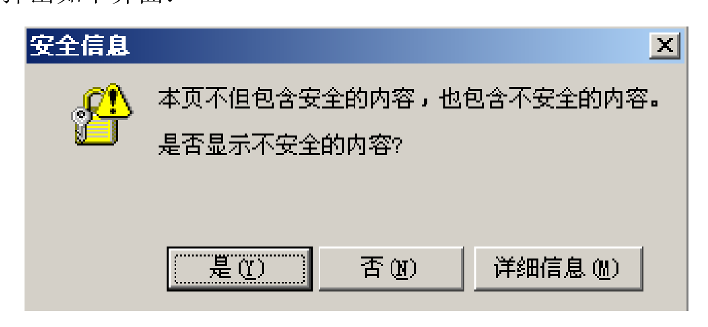
将ESV系列VPN防火墙的LAN口用一根网线联到本地的交换机上，或是直接联到一台普通PC的网卡接口上。将该PC的网卡IP地址设为192.168.0.X（X为1～253）网段，掩码为255.255.255.0，即可进行首次登录。

在 IE 的地址栏输入 https://192.168.0.254:10000 打开管理界面登录。

在进入登录界面前会弹出如下对话框，



点击“是”，会弹出如下界面：



点击“是”，就可以进入登录界面了，如下图：

默认登录界面用户名是“admin”，初始密码是“888888”。

在指定的用户名和密码输入框中输入用户名和密码，点击“登录”按钮，就进入 WEB 管理 VPN 防火墙主页了。

注　意:

VPN 防火墙的缺省密码是出厂时设置的。您也可以在 VPN 防火墙的修改帐号设置页面中修改密码。为了安全，我们强烈建议您务必在登录之后更改管理密码！密码请牢记，若是密码忘记，将无法再登录至 VPN 防火墙的设定画面，必须恢复到出厂值。

3.2 WEB 管理界面介绍

在页面左侧，本公司商标的正下方，是功能菜单界面，它呈树状目录结构；右下方大面积的区域是用于功能配置的主窗口。



左侧的功能菜单呈树状目录结构，整个目录分成两层，如果点击某一主项，就会展开这一主项下的所有子项；如果想要设置其子项，只需要点击相应子选项，主窗口就会切换到被点击子项的设置页。

在一个主项被展开的情况下，如果点击其它主项，以前展开的主项会闭合，被点击的主项将展开，此时主窗口仍然会显示上一次设置的子项的设置页，只有点击了新的设置子项，配置页面才会更改；如果点击已打开的主项，此主项会闭合，此时没有打开的主项，主窗口仍然会显示上一次设置的子项的设置页。由于受到网络速度和 VPN 防火墙工作负荷影响，可能菜单会将两次间隔时间较短的点击作一次点击来响应，此时只要注意适当延长点击时间间隔即可。



图：功能菜单

以下列出了功能菜单以及其子项：

系统信息：无

网口配置：模式选择、WAN 口配置、LAN 配置

网络配置：内网 DHCP、DDNS 配置、静态路由设置、虚拟 VLAN 设置、内网 IP 绑定

防火墙：设置选项、时间表、IP 管理、服务、端口映射、IP 地址映射、数据包控制策略

VPN 配置：VPN 配置列表、VPN 状态、PPTP 设置、PPTP 用户

流量管理：IP 流量控制、会话列表

服务管理：时间设置、命令行工具、系统升级、配置备份与恢复、恢复默认值

用户认证：WEB 认证设置、WEB 用户设置

日志管理：日志配置、系统日志、告警日志、审计日志

登录管理：无

修改账号：无

配置向导：无

重新启动：无

退出：　　无

📖 说明:

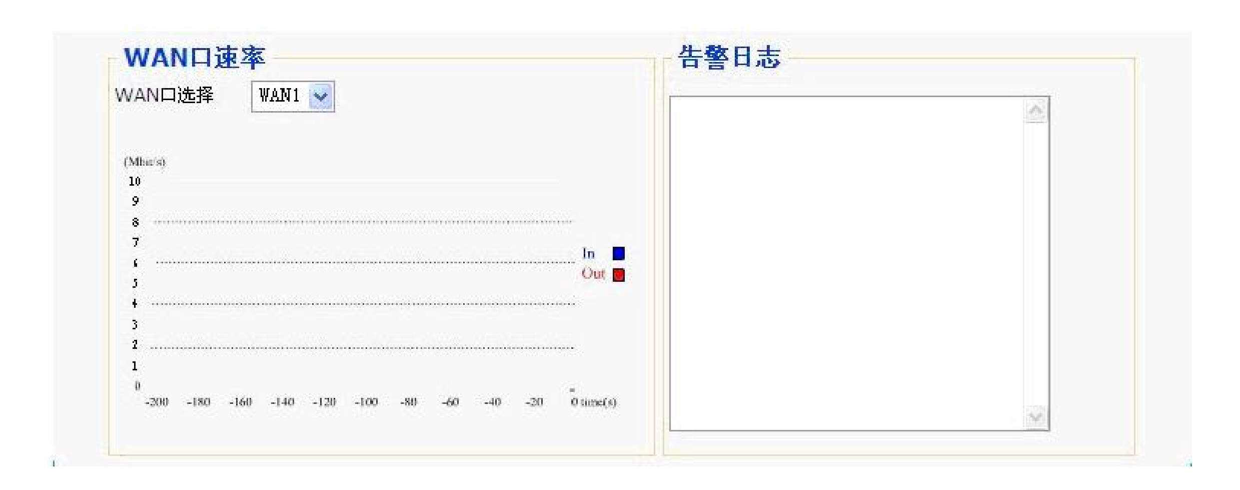
仅 ESV-3200 上具备用户认证的功能

📖 注意:

针对 VPN 防火墙设置所做的修改，只有在点击“保存”按钮（有些项目可能还需要 VPN 防火墙系统重启）后才会生效。

3.3 系统信息





- 系统信息：主要显示系统的相关信息如软件版本、以及当前的DDNS主机名、系统当前时间。
- 资源信息：主要本路由的资源信息，显示CPU负载、空闲内存、系统开机时间长和并发连接数。
- 接口信息：显示内网的IP以及WAN口IP以及端口的所有信息如内网、外网的流入、流出数据包的数据量。
- 用户信息：显示用户当前信息，主要有活跃用户数、DHCP用户数、PPTP用户数。
- 配置信息：显示用户配置的启动功能信息，有流量控制、DDNS设置、DHCP设置、攻击防范。
- WAN口速率：可以动态的通过页面显示出被选择WAN口当前的进出流量，能够动态的显示当前流量的状态。
- 告警日志：显示告警日志信息。

说明:

系统信息中的接口信息只显示当前已启用的有效WAN口及其信息，其他关闭的WAN口则不予显示。

系统信息中的系统时间只有在“服务管理”中的“时间设置”项中正确设置后才能反映正确时间。

3.4 网口配置

在“网口配置”菜单下面，有“模式选择、WAN1 口配置、WAN2 口配置内网配置”四个子项。单击某个子项，您即可进行相应的功能设置，下面将详细讲解各子项的功能。

3.4.1 模式选择

- 路由模式

选择路由模式，当VPN防火墙在起到VPN防火墙的功效时，假如和其它的路由器同在一个网络上运作，这里包括了一个分别处理上网的网关，假如选择路由模式，您需要设置另一个路由器作为网关，以便让接入的电脑也能够上网。



点击“保存”按钮保存选择的路由模式。使配置生效必须重新启动本机，点击“重启”按钮，等待重启完成，重新连接才能进入配置界面。

- 透明桥模式

透明桥模式是用来连通两个大型的网络。您的网络管理人应该填入网络段的信息，包括IP地址，子网掩码，和外置的网关地址。

- IP地址：　所有的WAN口和LAN口会分享这个IP地址。
- 子网掩码：所有的WAN口和LAN口会在这个子网里。
- 外置网关：外置网关指的是已在网络内部运行且被设置为网关的设备。
- NAT模式: 从WAN口出去的数据会被NAT成此处配置的IP地址.
- 带宽：

- 上行带宽：此 WAN 口分配上行数据的速率。VPN 防火墙默认值为 102400k bps(100M)。这一配置对上行数据缓存调节和权重来说很重要。如果你使用上行速率为 0.5Mbps 的 DSL 服务，那么上行速率设置为 500K bit/s。
- 下行带宽：此 WAN 口分配下行数据的速率。VPN 防火墙默认值为 102400k bps(100M)。这一配置对下行数据缓存调节很重要。如果你使用下行速率为 2Mbps 的 DSL 服务，那么下行速率设置为 2000K bit/s。

您当前的位置是：模式选择

帮助

模式

路由模式

透明桥模式

IP地址

子网掩码

外置网关

带宽(kbit/s)：上行　下行

NAT模式

网关模式

重 启　保存

注意：1.当您网络设置为透明模式时，将清除原先的LAN/WAN口IP设置。

2.模式选择改变后，必须重启系统，新设置才能生效。

点击“保存”按钮保存选择的透明桥模式。使配置生效必须重新启动本机，点击“重启”按钮，等待重启完成，重新连接才能进入配置界面。

- 网关模式

当VPN防火墙在起到路由器的功效时，一般的宽带连接使用网关模式。



如果使用多条同一运营商的 ADSL,可以选择自动负载均衡，则不需要在 wan 口配置中使用静态路由表，流量会自动使用多 wan 口传递数据，如果既不选择自动负载均衡,也不设置 wan 口的静态路由表,在多 wan 的环境中,wan1 为主线路,其他 wan 口线路则为备用线路， 如果在 wan 口配置静态路由表,则变为策略路由模式，流量会根据路由表来选择走那条线路，则点击“保存”按钮保存选择的网关模式。使配置生效必须重新启动本机，点击“重启”按钮，等待重启完成，重新连接才能进入配置界面。

3.4.2 WAN 口配置

设定WAN口的配置信息。先选择对应的WAN口进行配置，然后再输入相应的参数即可。



- WAN 口的选择：可以对 WAN 口进行选择，分别定义 wan1-wan2 的设置

- 配置方法：　　用户可以根据自己的实际连接方式进行选择“静态 IP、ADSL 拨号连接、DHCP 连接、DHCP+连接，关闭连接”等几个选项。
  - 静态 IP 配置选项：　静态 IP 时，由 ISP 提供相应的 IP 地址，DNS 必须手动填写。

静态IP配置选项:

IP地址　　　　DNS服务器1

网络掩码　　　DNS服务器2

默认网关　　　DNS服务器3

(如果不设置DNS服务器,系统将不进行断线检测)

  - 拨号连接配置选项：　ADSL 拨号连接，连接时的用户上网账号和密码由当地 ISP 供应商提供。
    - 登录用户名：输入当地 ISP 供应商提供的用户名。
    - 使用密码登录：输入当地 ISP 供应商提供的密码。
    - 从 ISP 得到 DNS 配置：选择是否要从 ISP 供应商处自动获得 DNS 服务器。
    - 特殊模式：针对部分有路由受限问题地区的用户。
    - 是否限制包尺寸：选择是否限制包尺寸选项。
    - 是否进行 LCP 检测：ADSL 的断线检测。



➢ DHCP 连接：直接由 ISP 提供商进行动态的 IP 地址分配。

➢ DHCP+连接：为解决特殊地区的 DHCP+接入方式，需要输入此方式的用户名和密码。



➢ WAN 的静态路由：显示手动设置的 WAN 口的静态路由表项，静态路由的表达格式为：202.104.25.33/16，前者为目的 IP 地址或网段，后面为 32 分段表达方式子网掩码，16 对应的子网掩码为 255.255.255.0（可以参考说明书附录 B 分位表示法的表格）。

➢ 带宽管理：

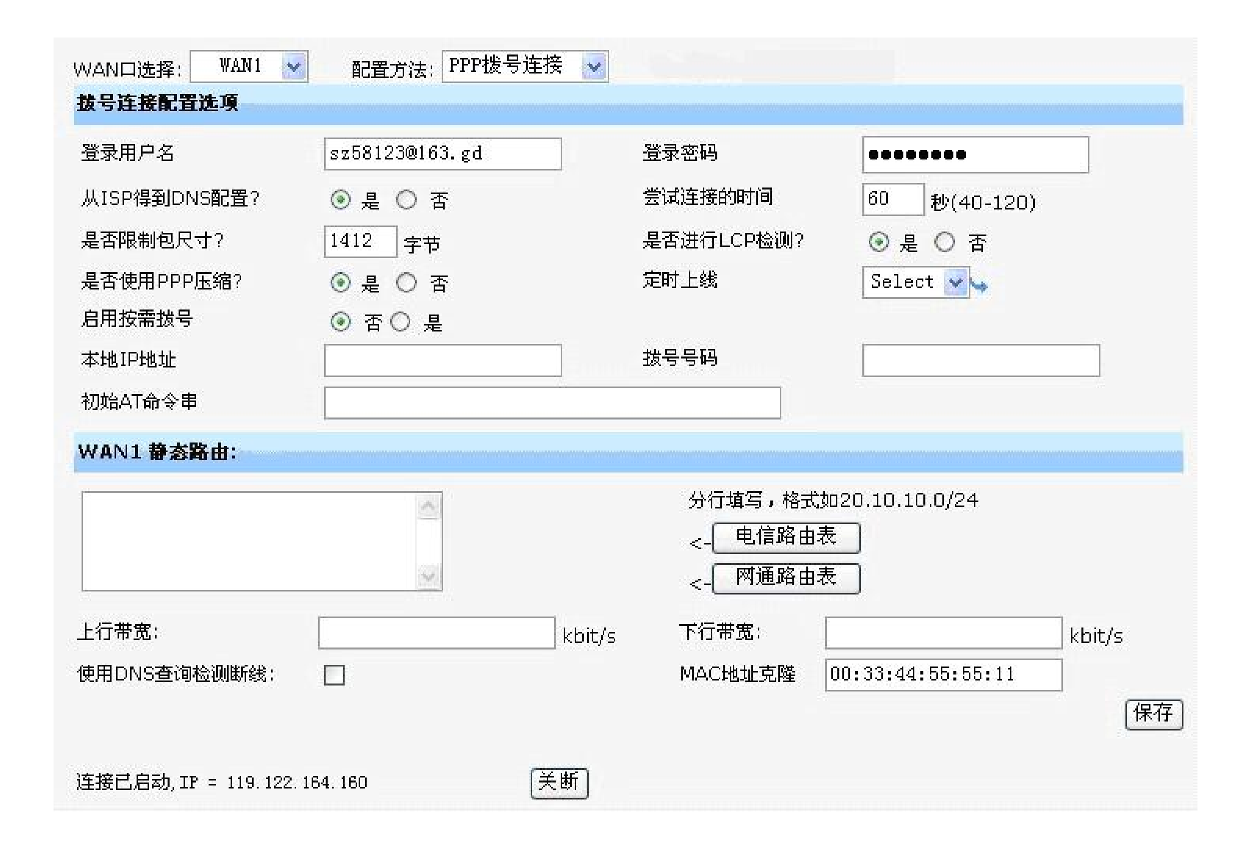
● 上行带宽：此为 WAN 口分配上行数据的速率。路由器默认值为 102400k

bps(100M)。这一配置对上行数据缓存调节和权重来说很重要。如果您使用上行速率为 0.5Mbps 的 DSL 服务，那么上行速率设置为 500K bit/s。

- 下行带宽：此 WAN 口分配下行数据的速率。路由器默认值为 102400k bps(100M)。这一配置对下行数据缓存调节和权重来说很重要。如果您使用下行速率为 2Mbps 的 DSL 服务，那么下行速率设置为 2000K bit/s。

提示：WAN 口带宽管理只有在选用流量管理中的最小带宽管理或启用系统流量阀值才可生效。

- 断线检测：对于静态 IP 和 DHCP（动态 IP）接入方式如果需要检测连接状态，可以选择此项。
- MAC 地址克隆：可以更改路由器 WAN 口的 MAC 地址。



以上配置只有在重启后才能生效。

📖 什么是 DNS?

DNS 是域名系统 (Domain Name System) 的缩写，该系统用于命名组织到域层次结构中的计算机和网络服务。DNS 命名用于 Internet 等 TCP/IP 网络中，通过用户友好的名称查找计算机和服务。当用户在应用程序中输入 DNS 名称时，DNS 服务可以将此名称解析为与之相关的其他信息，如 IP 地址。因为，你在上网时输入的网址，是通过域名解析系解析找到相对应的 IP 地址，这样才能上网。其实，域名的最终指向是 IP。

比如您在浏览器中输入 www.163.com，那么 DNS 服务器将会将此域名解析成类似于 218.107.213.22 的 IP 地址，由于 ISP 的服务差异，使得每次解析结果都不一定相同。

3.4.3 LAN 配置

LAN 口地址配置及网段参数；依照用户需求设定。示例：

内网配置：
LAN编辑
IP地址 192.168.0.254
子网掩码 255.255.255.0
MAC地址 00:e0:11:13:44:23

- IP地址：VPN安全网关对于内网的IP地址。
- 子网掩码：内网的IP掩码。
- MAC地址：LAN口的MAC地址。

此处设置的VPN安全网关内网IP与内网DHCP设置的网关IP保持一致，点击“保存”按钮后会提示用户“LAN口IP已修改，是否重新配置DHCP”，点击“是”将跳转到DHCP配置页面。使配置生效必须重新启动本机，等待重启完成，重新连接按照更改后的IP地址才能进入配置界面。

3.5 网络配置

3.5.1 内网 DHCP

DHCP服务器默认值是开启的，开启DHCP服务器功能可以提供局域网络内的计算机自动取得

IP的功能，（如同NT服务器中的DHCP服务），好处是每台PC不用去记录与设定其IP位置，当计算机开机后，就可从VPN安全网关自动取得IP地址，管理方便。

DHCP服务配置

☑ 打开DHCP服务

网关IP		(可选)
DNS服务器		(可选)
内网IP地址起点	192.168.0.10	
内网IP地址终点	192.168.0.250	
内网IP网络掩码	255.255.255.0	
租期		小时

☐ 自动应用于绑定MAC地址的IP用户
启用该功能后, 在用户管理或内网绑定中设置的用户将分配你设置的IP

☐ 启用自动绑定IP/MAC功能
启用该功能后，将自动启动内网MAC/IP绑定和允许新用户连接功能，
这时只允许用户通过DHCP方式连接进来，如果有计算机通过DHCP获得IP，那么他的IP/MAC信息将自动绑定。

确定　查看DHCP列表

- 打开DHCP服务器：开启DHCP功能，使VPN安全网关作为DHCP Server为局域网自动分配IP地址。
- 网关IP：该设置为默认VPN安全网关对局域网的IP地址。该IP地址出厂设置为**192.168.0.254**，用户可以根据需要改变它。
- DNS服务器：手动输入DNS服务器地址后，DHCP服务器将此DNS服务器地址分配给PC。
- 内网IP地址起点：该设置为VPN安全网关的DHCP服务器为局域网内电脑分配IP地址时开始的值，若设置为192.168.0.2.也就是说，第一台向VPN安全网关发出DHCP申请的电脑，获取的IP是192.168.0.2，第二台则会是192.168.0.3.依此类推。如果需要，您可以改变该数值。
- 内网IP地址终点：该设置为VPN安全网关的DHCP服务器为局域网内电脑分配IP地址时最后的值。若设置为192.168.0.150，则IP地址从开始值分配至此值时，即不再分配IP地址。
- 内网IP网络掩码：该设置为VPN安全网关对局域网的子网掩码。
- 租期：DHCP服务器所分配的IP的一个租约时间。
- 自动应用于绑定MAC地址的IP用户：此选项可以使得在DHCP服务打开时，PC的MAC地址和

所获取的IP有确定对应关系，而不是递加和随机的，遵循IP+MAC地址绑定中的原则（第3.5.5章节）。

- 启用自动绑定IP/MAC功能：启用该功能后，将自动启动内网MAC/IP绑定和允许新用户连接功能，这时只允许用户通过DHCP方式连接进来，如果有计算机通过DHCP获得IP，那么他的IP/MAC信息将自动绑定。
- 查看DHCP列表：点击此按钮，会列出DHCP服务器分配的IP的详细信息。

注 意:

1. 为了使用本 VPN 防火墙 DHCP 功能，局域网中计算机的 TCP/IP 协议必须设置为“自动获取 IP 地址”。
2. 设置完成后，请点击“确定”按钮使用户的设置生效。
3. 当WAN处于拨号模式且没有从ISP处获取DNS服务时，可在此处填入DNS服务器地址，且需与“DNS&DDNS配置”中DNS服务器设置第一栏保持一致。
4. “自动应用于绑定MAC地址的IP用户”功能启用后，DHCP自动分配的IP会将遵循IP与MAC地址对应表中的规则，如果你将某IP与某MAC地址进行了绑定，那么此MAC地址所属的网卡只能分配到该IP。（第3.5.1章节）。

3.5.2 DDNS 配置

DDNS（动态DNS）服务让您分配一个固定的网域名给一个动态WAN IP地址。

在还没有设置 DDNS 之前，您需要访问 WWW.DTDNS.COM， WWW.3322.org 或其它的 DDNS 服务商并且注册一个网络域名。(DDNS 服务是 DTDNS.COM 等服务商提供的）在其中的动态域名当中添加一个您当前网络的主机名。然后在这里将对应的信息填写进去。

DDNS 服务：在默认下 DDNS 功能是没有启动的。要激活此功能，只要从下拉式菜单中选择一个 DDNS 服务商，并且在您和 DDNS 服务商设置的帐户里输入用户名，密码，和主机名。

选择启动 DDNS 后，每次拨号连接都会自动更改本域名的 IP 地址，则客户端即可通过动态域名访问到服务器。

您当前的位置是：DDNS 配置

帮助

动态DNS选项

DDNS序号 DDNS1

启用DDNS1

WAN口选择 默认

动态dns服务商 3322.org

主机名1

DDNS的用户名1

DDNS的密码1

保存

- DDNS序号：选择你当前所需要定义的DDNS。
- 启用DDNS：是否启用此功能。
- WAN口选择：选择您所需要定义的WAN口。
- 动态DNS服务商：可以选择3322.org、dtdns.com、congle.com、vier.cn、webddns。
- 主机名：向DDNS服务提供者所申请的本设备的主机名称，如：router123.3322.org。
- DDNS的用户名：向DDNS所注册的账号用户名。
- DDNS的密码：向DDNS服务提供者所申请的与用户名名称对应的密码。
- 保存：按下此按钮“保存”即会储存刚才所变动的修改设定内容参数。

3.5.3 静态路由设置

通过配置静态路由，用户可以人为地指定对某一网络访问时所要经过的路径， 在网络结构比较简单，且一般到达某一网络所经过的路径唯一的情况下采用静态路由。

假如好几个路由器连接到您的网络，为了确保您方便快捷的与那几个路由器所在网络的通讯，您需要配置静态路由。静态路由的功能决定数据在您网络上流动的路线。静态路由让不同的IP网域用户经过路由访问Internet。这是一个高级的功能，请小心地进行。



点击“新增”按钮增加一个路由表格。输入下面的数据，创立静态路由表格：



- 目的地IP：输入目的LAN 分段的网络地址。
- 子网掩码：输入目的地LAN IP网域的子网掩码。基于IP 网域标准，子网掩码是255.255.255.0或其他设定的值。
- 默认网关：假如远端路由是用来连接网络到互联网，那么网关的IP是远端路由的LAN IP地址。点击：“保存”按钮保存静态路由设置。

3.5.4 虚拟 VLAN 设置

这里所谓的虚拟VLAN，就是在单个网络接口上绑定多个虚拟接口和不同的网段。也就是说，被VLAN隔离的用户可以同时接到单个网络接口，在经过网关上网访问的同时，也可以在不同的VLAN之间彼此互访。因为路由器虚拟VLAN接口在用户上网的同时可以成为VLAN用户之间互访的桥梁，额外的网络接口就不需要了。

您当前的位置是：VLAN设置

网络地址	子网掩码	网络接口	操作

页码：1/0 上一页 下一页 新增

点击“新增”按钮增加VLAN设置。输入下面的数据，创立新的VLAN设置：



- 网络地址：输入需增加的网络地址或地址段。
- 子网掩码：输入需增加的网段的子网掩码。
- 网络接口：从下拉式菜单中选择一个桥梁端口：透明桥、LAN，WAN1或WAN2。

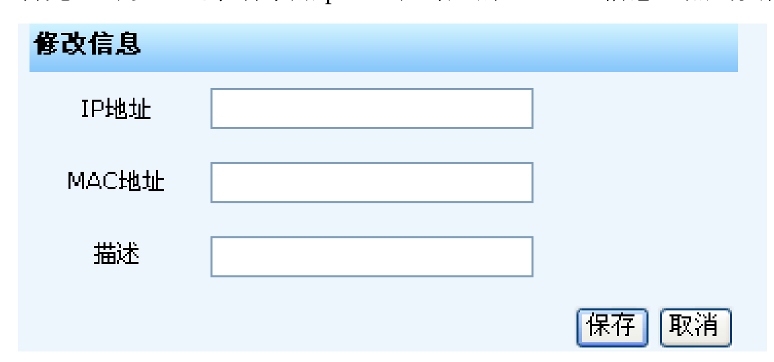
点击“保存”按钮保存VLAN 设置。

3.5.5 内网 IP 绑定

用户可以在LAN口上绑定多个内网IP地址和其对应的MAC地址，还可对绑定IP进行增减操作，在绑定的IP栏里面可以查看IP对应的绑定地址。有效的防御了ARP病毒，也方便了网络管理者对内网的管理。



首先，可以通过手动添加ip地址和对应的mac地址信息，点击页面下面的新增：



填写相关的pc机的IP地址和MAC地址信息以及描述信息，点击保存后，会自动显示在绑定列表中。



- 启用：勾上使内网IP绑定生效。
- 绑定列表：此列表显示了绑定信息，可以通过“新增”逐个添加绑定的IP和MAC地址。
- 批量绑定：在此方框中既可手动输入内网绑定的IP与MAC地址，可一次输入多个，格式如框图右边注释所示。注意每行一条。也可以点击“arp列表”自动扫描出当前的IP-MAC表，直接点击“复制”按钮将自动粘贴到方框中。如图例：



- 允许新用户连接：勾上则新接入的用户仍然能够正常上网。不勾则必须是在IP绑定列表中绑定用户才能上网，新用户需要上网必须添加到绑定列表中方可上网。
- 输入完毕之后，点击“保存”按钮保存列表。

3.6 防火墙

3.6.1 设置选项

从防火墙功能的一般设定选项当中，您可以控制开启(Enable)或是关闭(Disable)这些选项功能。

防攻击 选项

- ☐ 禁止本机被Ping
- ☐ 禁止本机被外网访问
- ☑ 过滤 SYN 攻击　阈值: 包/每秒　已过滤 : 0 包
- ☐ 过滤 UDP 攻击　阈值: 包/每秒　已过滤 : 包
- ☑ 过滤 Tear Drop 攻击　已过滤 : 包
- ☑ 过滤 IP Spoofing 攻击　已过滤 : 0 包
  用于过滤一些假冒源地址对路由器的攻击，更精确的过滤需要配合MAC/IP绑定来实现。
- ☑ 常见攻击特征防范　已过滤 : 包
- ☑ 过滤 Ping of Death 攻击
- ☐ 使用IP策略控制所有包(否则只控制新建连接)
- ☐ 限制用户每秒新建连接数　最大: 30 (10-40)　已过滤 : 包
  启用此功能同时启用防范攻击，如果用户新建连接数超过限制数，则会被断开2分钟，用于防范P2P下载和病毒攻击。
- ☑ 广播arp信息(防止arp欺骗)速度　2 个/秒(1-30)
- ☐ LAN口MTU值
- ☐ TCP MSS值
- ☐ 启动snmp服务
  snmp绑定到LAN口IP，需要通过外网访问时要创建一个端口映射到LAN口IP。
- ☐ 启动UPNP功能　查看UPNP列表

确定

➢ DOS 保护

为了保护内网，在这里您可以设定阻止从 Internet 来的攻击，例如 SYN 攻击，UDP 攻击，Ping of Death 和 Tear Drop 等，并设置相应参数。

➢ 禁止本机被外网ping及禁止本机被外网访问

前者选择后外网ping路由器的WAN口IP将无法ping通，后者选择后将无法通过WAN口IP访问管理路由器。

➢ 过滤IP Spoofing攻击

即保护内网免受IP欺骗攻击。

➢ 常见攻击特征防范

➢ 过滤常见的攻击包，例如根据tnk2k，ddoser等的指纹特征进行防范。

➢ 使用IP策略控制所有包

启用后，会对新建的连接和已经启用的会话连接都进行策略控制。

➢ 限制用户每秒新建连接数

在我们用电脑工作时，打开的一个窗口或多个 Web 页面需要建立一个或多个 IP 连接，每一个 IP 连接我们可以把它叫做一个“会话”，扩展到一个局域网里面，所有用户要通过防火墙上

网，要打开很多个窗口或 Web 页面（即将产生更多数量的会话），那么，这个防火墙，所能处理的最大会话数量，就是“并发连接数”。

限制单个用户的并发连接数是为了防止病毒伪装“会话”而造成对网关的攻击。默认的最大单个用户的并发连接数是 30。

- 限制非授权用户访问路由器（通过策略控制）

  在没有选择此项时，无论您在数据包控制策略中做任何设置，内网的任何PC都能进入路由器的WEB管理。在选择此项之后，您可以通过数据包控制策略来授权部分用户能管理路由器，部分用户不能管理路由器。

- 广播ARP信息（防止ARP网关欺骗）

  每秒钟发送一次网关的IP与MAC地址信息广播包。为了保证局域网中的电脑不被感染病毒和木马的电脑欺骗，可以选中此项，使得每台电脑能获得正确的网关信息。

- LAN口MTU值

  对LAN口数据包转发的数据包最大传输单元进行限制。

- TCP MSS值

  TCP数据包每次能够传输的最大数据分段。

- 启动snmp服务

  启用此服务能够在LAN的PC中启用SNMP管理路由器。

- 启动UPNP功能

  选择此项后，路由器将启用“通用即用”协议能够自动发现网络中的UPNP设备，实现自动的端口映射。

- 日志服务器地址：在日志服务器地址栏中填入日志服务器的IP就可以保存路由器中的日志，；路由器重启后在PC上也能保存，为以后的查询工作，解决问题提供便利。

注意:

在日志服务器地址栏中填入日志服务器的IP之外，还必须在PC上安装一个日志信息接收端。

3.6.2 时间表



时间表是服务于防火墙中的数据包控制策略的，在数据包控制策略中，您可以通过定义时间表来实现数据包控制策略只在某一个时间段实现。具体时间表分为以下两种，可以点“增加”来进行添加：



- 名称：定义此条时间表格的名称，在数据包控制策略中可以选择到您定义的时间表。
- 启用循环操作：以星期为单位，按星期一至星期天每天的时间来定义时间段，循环操作。
- 启用单次操作：以时间起始定义时间表，从1970至2037年内的任意时间段，单次操作。

3.6.3 IP 管理

对用户名及IP等进行定义，方便管理，也可以在数据包控制策略中对您所定义的IP及IP段进行策略控制。可以定义一个用户，也可以定义一组用户，一段IP用户，也可以定义单个域名或者外网IP。用户定义后即可针对该用户设定相应的防火墙规则。当所定义的用户已被防火墙规则使用时，要删除该用户必须在删除对应防火墙的规则后，才恩、被删除。下图为本说明示例：



点击“创建”可新建用户，点击用户名可以对已有的原用户进行编辑：



- 名称：用于区分所定义的IP或者IP段。定义必须是单一不重复的
- 单个IP：可以从ARP列表中直接提取信息，也可以根据用户自己的要求填写某个IP和对应的MAC地址
- 一组IP：则是通过更改子网掩码来定义一个IP，例如：192.168.0.0 子网掩码：255.255.255.0 则表示了 192.168.0.1-192.168.0.254整个C类地址网段
- 一段IP：则是起始和终止IP来定义，如：192.168.0.1-192.168.0.100
- 其他IP或域名：主要是用以定义外网的IP及域名，方便在数据包控制策略中进行选择。

3.6.4 服务

对网络端口进行定义，以便于管理。可以定义数个端口，也可以定义一段连续的端口。端口定义后即可针对该用户设定相应的防火墙规则。当针对端口设定了相应的防火墙规则后，则不能再直接删除所定义的端口，如需删除，需先删除定义的规则。

在这里，端口的定义分为缺省和手动2部分，缺省为不能更改的，系统已经定义好的端口。在手动中，您可以定义一些您需要的端口或者端口段。下图为本说明示例：



您当前的位置是：服务

缺省 手动

序号	服务名	端口范围	协议	操作
1	NetMeeting	1720	TCP/UDP	
2	PPTP	47,1723	TCP/UDP	
3	SNMP	161-162	TCP/UDP	
4	NTP	123	TCP/UDP	
5	UDP	0-65535	TCP/UDP	
6	QUAKE	26000,27000,27910,27960	TCP/UDP	
7	AOL	5190-5194	TCP/UDP	
8	INFO_ADDRESS	17	TCP/UDP	
9	IKE	500	TCP/UDP	
10	HTTPS	443	TCP/UDP	

页码： 1/5　1　跳转　上一页　下一页

若需要定义新的端口或者端口段的服务，则点击“手动”：

您当前的位置是：新增服务

服务设置

服务名* 协议 TCP/UDP

端口号 起始 0 终止 65535 （端口范围）

第1个 第2个 第3个 第4个 第5个 第6个 第7个 第8个 第9个 第10个 （单个填写，至少填写第一个）

保存

- 服务名：您所定义的服务名称；可以使用英文、数字，中文来命名。
- 端口号：您可以定义一个端口段（起始端口-终止终止端口范围内）

  组合的端口号组（可以是一个或者多个，每一个服务组合端口不多于十个）

3.6.5 端口映射

端口映射用于建立web 站点、Email、FTP等内网服务器到外网的映射，使外网可以使用此服务。

端口映射功能被用来在网络上设置公共服务。当在您网络外的用户（Internet上的用户）向您的网络提出请求，端口映射能转发那些请求到已装备好处理这些请求的电脑。例如说，您转发端口号80（HTTP）到IP地址192.168.1.100，那么所有从外而来的HTTP请求会被转发到192.168.1.100。

您可以使用此功能经由IP网关建立Web站点、Email、FTP服务器等服务。例：将192.168.1.1的Server 端口80映射为WAN口公网IP的8080端口，您就可以通过http://WAN的IP：8080来访问192.168.1.1这台PC上的WEB服务器。

确定您输入了一个有效的IP地址。（为了适当地操作一个Internet服务器也许您需要在服务器上使用静态的IP地址）为了增加安全，那些在您网络之外的（例如Internet）用户会能够和服务器相通，但他们事实上不会直接连接到服务器。那些信息包只是经过转发而已。

您可以通过修改和删除对您已经定义好的端口映射进行编辑和删除。



- 端口范围：您所定义的外网端口；外网端口用户通过此端口范围访问内网服务器。
- 映射端口范围：您所映射的内网服务器端口；内网服务器提供服务的端口。
- 服务器：空白默认为 WAN 口 IP
- 映射服务器：内网服务器的IP；内网服务器一般使用静态IP才能确保每次正确提供服务。
- 协议：可以选择包括(TCP/UDP)

例：您在192.168.0.98这台PC上架设了FTP服务器，您只需要做如上设置，您就可以通过外网的IP来访问192.168.0.98这台PC上的FTP服务器。（服务IP默认为当前的外网IP）。

3.6.6 IP 地址映射

Internet网络不能直接寻址到IP地址，必须经过一定的转换才能将内网IP地址映射为Internet网络的物理地址.例如：将外网的IP 地址（59.173.89.191）直接映射到内部服务器的IP 地址（192.168.0.5）让外网用户可以充分利用内部网络的资源。



例如：外网IP：59.173.89.191直接映射到内部服务器192.168.0.5，外网的用户就能通过59.173.89.191这个IP访问到内部服务器192.168.0.5。

您若要编辑IP地址映射，点击在操作栏里的“修改”按钮。也可以将其删除。



提示：服务器IP地址为有效的外网的IP地址，此地址必须在WAN接口出现过，否则将会无效。映射服务器填写内网的服务器IP地址。

3.6.7 数据包控制策略

您可以在这里通过定义不同的访问规则，来实现对内网的用户的管理，还可以组合规则，实现内网用户不同的权限。

注意：序列号数字小的规则优先起作用，当检测到数据包符合某条规则后，该规则被执行，防火墙将不再检测后续规则。“内网IP”“外网IP”“服务”需要在之前的“IP管理”“服务”项中进行定义。以及访问规则中出现的“时间表”，也需要在之前的“时间表”项中进行定义。



提示：设定了多条数据包策略后，点击“使配置生效”即可生效；且序列号数值越小，规则优先级越高，将被优先执行，并忽略后面的规则。

例：1.您定义了一条规则，内容为内网所有用户都能上www.sina.com.cn这个网站，序列号为“010”。

2.您再定义一条规则，内容为内网所有用户都不能上外网，序列号为“020”。

规则生效后，内网的所有用户将不能上其他外网，但是都可以访问www.sina.com.cn。

帮助

访问规则

☑启用

序列号* （序列号小则优先级高。）

☑内容过滤启用

内容过滤 ⦿数据包 ○域名 ○文件后缀名 ○所有域名

应用层处理 ○封锁 QQ ○封锁 MSN ○P2P ○WEB行为日志 ○非标准HTTP请求

说明： 1.选“域名”时，可匹配完整或部分域名，可以填写多个，以空格隔开；
2.选“非标准HTTP请求”时可过滤非HTTP标准程序通过80端口通讯；
3.选“文件后缀名”时的填写格式如：*.bat *.exe *.doc，以空格分隔。

规则配置

方向 内网->外网

内网IP 请选择

外网IP 请选择

服务 请选择

IP类型 请选择

时间表 请选择

说明： 1.带宽控制，控制这条策略每个IP的最大带宽，选择时，超出带宽的包将被拒绝；
2.时间表，即此条规则只应用于所选的时间段中有效；
3.当某项不选择时，代表该项不做限制。

策略

带宽/路由策略 通过策略

通过策略 ⦿通过 ○通过并日志 ○拒绝 ○拒绝并日志

说明： 1.通过：允许该数据包通过，不记入日志；
2.拒绝：拒绝该数据包通过，不记入日志；
3.日志：记入日志，并继续执行下条规则。
4.拒绝并日志：拒绝该数据包通过，并记入日志；
5.外网线路：让该数据包走特点的外网口。

注意：带*的为必填项

保存

- 序列号：序列号小则优先级高，如“001”号的规则将先于“002”号的规则执行。
- 内容过滤：当选择到“数据包”时，内容为关键字符的过滤。

  当选择到“域名”时，可以填写完整或部分的域名，可以写多个，以空格隔开。

  当选择到“文件后缀名”，填写格式为：.bat .exe .doc 中间以空格隔开。

  当选择到“所有域名”，过滤所有域名。

当选择到“封锁QQ”时，通过定义可以让内网用户不能上QQ。

当选择到“封锁MSN”时，通过定义可以让内网用户不能上MSN。

当选择到“P2P”时，通过定义可以让内网用户不能使用P2P。

当选择到“WEB行为日志”时，可以在系统日志中看到通过WEB上网的行为日志。

当选择到“非标准HTTP请求”，可以过滤非HTTP标准程序通过80端口进行通讯。

- 方向： 内网到外网，外网到内网，定义的是这个规则的方向。
- 内网IP：可以在这里选择到您在“IP管理”中定义的IP，IP段或者IP组。
- 外网IP：可以在这里选择到您在“IP管理”中定义的外网IP或者名称。
- 服务： 可以选择任意服务项，也可以选择在“服务”中您定义的项目名称。
- IP类型：包括 ALL，TCP，UDP。（ALL为TCP+UDP）
- 带宽控制：控制这条策略每个IP的最大带宽，当超过了带宽的数据包会拒绝。（在流量控制中的定义优先于此处的设置）
- 时间表：可以在这里选择您在“时间表”项中定义的时间表项名称。
- 当以上条件符合时：

选择通过，数据包符合所定义的规则时将直接允许通过。

选择拒绝，数据包符合所定义的规则时将直接被拒绝。

选择日志，数据包符合所定义的规则将在“系统日志”中显示出来信息。

选择拒绝并日志，数据包符合所定义的规则将被拒绝，并在“系统日志”中显示出来。

选择WAN，所定义的规则的数据以您所选择的WAN口作为出口。

3.7 VPN 配置

3.7.1 VPN 配置列表

您当前的位置是： VPN配置列表

连接	用户名(ID)	内网用户	对方IP	外网用户
1.服务器(编辑)	guangzhou	192.168.1.0/255.255.255.0	动态IP	广州
2.客户端(编辑)	test.21door.com	192.168.1.0/255.255.255.0	test1.21door.com	上海
3.客户端(编辑)	test.21door.com	上海	202.96.254.254	10.0.3.0/255.255.255.0
4.服务器(编辑)	guest	192.168.1.0/255.255.255.0	动态IP	私有网段客户端

增加VPN配置 ◉客户端 ○服务器端 ○客户端软件服务器

网络设置 选项

☑ VPN用户虚拟为本机IP

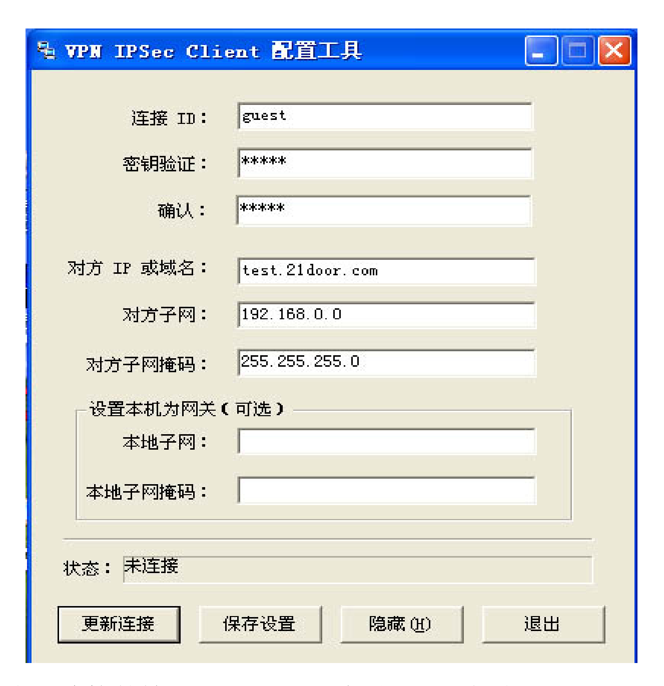
☑ 支持VPN隧道转发

确定

上图共有四条配置：

第一条：分支机构（guangzhou）作为子网通过同类型设备通过VPN 接入本网。

第二条：设定移动用户用guest 作为帐号登陆进来。本系统同一VPN 帐号，可同时联接多个用户，如本例中，可以多人同时使用guest 帐号登陆进来，也可以在系统中设置不同的帐号归不同人使用。移动办公用户，可以在其电脑（win2000，Win2003，或winXP 操作系统）上，安装配套的VPN 客户端软件，其客户端登陆界面设置如下：



点击更新连接，状态为已连接的情况下，即可登陆到公司网络上，进行远程办公。

第三条：本设备作为客户端，连接使用动态域名的test1.21door.com（上海子网）。

第四条：本设备作为客户端，连接使用固定IP 的其它设备。

需要说明的是在VPN 的网络中，可以把多个子网联系到一起， 路由是靠子网的地址来区分的，所以所有连进VPN SERVER 的客户端的子网不能冲突，也不能与服务器端的子网冲突。

1) 增加VPN客户端

用本设备作为客户端，来主动的连接其它设备,从而进入其局域网。如图：

您当前的位置是：编辑客户端VPN配置

用户名(本地ID) test.21door.com
本地子网 选择 上海
IP值
掩码
对方IP或域名 202.96.254.254
对方子网 选择 输入一个
IP值 10.0.3.0
掩码 255.255.255.0
密码 ******
高级

本地ID是此连接的用户名
(默认使用本机名)
ID和密码与服务器中的相等,即可建立
建议的名字如 : client1.vpn11.cor

注意:
在VPN 的网络中，可以把多个子网
联系到一起，路由是靠子网的地址
来区分的，所以所有连进VPN SERVE
的客户端的子网不能冲突，也不能
与服务器端的子网冲突。

模式选择	主模式
IKE	加密算法 3DES 认证 MD5 DH组 DH2
ESP	加密算法 3DES 认证 MD5
PHASE 1	秒
PHASE 2	秒
保持活跃	☑
压缩	☐ (Support IP Payload Compression Protocol(IPComp))

确认

保存并生效 新建并生效 删除 取消

用户名（本地ID）：即所要连接的VPN服务器分配给主动连接方的账户。

本地子网：即本地VPN 连接的用户地址信息。

对方子网：对方的子网信息。

对方IP 或域名：所要连接的VPN 服务器的信息。

模式选择：选择加密模式，加密算法等。设置的模式与加密算法需要与对方一致。

2) 增加VPN服务器

将本设备作为服务器，增加账号，使得其它用户能连接进来。其配置界面如图：

您当前的位置是：编辑服务器端VPN配置

用户名(对方ID) guangzhou
本地子网 选择 输入一个
IP值 192.168.1.0
掩码 255.255.255.0
对方IP或域名 动态IP
对方子网 选择 广州
IP值
掩码
密码 ******
高级

对方ID是此连接的唯一标志
(既对方机器名)
ID和密码与客户端中的相等,即可建立联接
建议的名字如 : client1.vpn11.com

动态IP表明对方可能是拨号连接,不用输入

注意:
在VPN 的网络中，可以把多个子网
联系到一起，路由是靠子网的地址
来区分的，所以所有连进VPN SERVER
的客户端的子网不能冲突，也不能
与服务器端的子网冲突。

模式选择	主模式				
IKE	加密算法 3DES	认证	MD5	DH组	DH2
ESP	加密算法 3DES	认证	MD5		
PHASE 1	秒				
PHASE 2	秒				
保持活跃					
压缩	(Support IP Payload Compression Protocol(IPComp))				

用户名（对方ID）：分配给登录方的的账户。

本地子网：即对方登陆后，可连通本公司的用户设定。

对方IP 或域名:登陆方的IP或域名，当要连进的用户为动态IP 时，则不需输入。

注意：需要通过VPN 登陆进来的用户一定要和本处VPN设定的数据一致才能接通。

对方子网：当连进来的用户为一子网时，一定要选择其对应的子网数据。可以在网络用户管理内定义好，亦可在此输入。

模式选择：选择加密模式，加密算法等。设置的模式与加密算法需要与对方一致。

3） 增加客户端软件服务器

提供给移动办公用户，用户可以在其电脑（win2000，Win2003，或winXP 操作系统）上，安装配套的VPN 客户端软件接入VPN.

您当前的位置是：编辑服务器端VPN配置

用户名(对方ID) guest

本地子网 选择 输入一个

IP值 192.168.1.0

掩码 255.255.255.0

对方IP或域名 动态IP

对方子网 选择 私有网段客户端

IP值

掩码

密码 ******

高级

对方ID是此连接的唯一标志
(既对方机器名)
ID和密码与客户端中的相等,即可建立联接
建议的名字如 : client1.vpn11.com

动态IP表明对方可能是拨号连接,不用输入

注意：
在VPN 的网络中，可以把多个子网
联系到一起，路由是靠子网的地址
来区分的，所以所有连进VPN SERVER
的客户端的子网不能冲突，也不能
与服务器端的子网冲突。

模式选择	主模式
IKE	加密算法 3DES 认证 MD5 DH组 DH2
ESP	加密算法 3DES 认证 MD5
PHASE 1	秒
PHASE 2	秒
保持活跃	
压缩	(Support IP Payload Compression Protocol(IPComp))

确认

保存并生效 新建并生效 删除 取消

用户名（对方ID）：即所要连接的VPN服务器分配给主动连接方的账户。

本地子网：即本地VPN 连接的用户地址信息。

对方子网：默认为私有网段客户端(不可配)。

对方IP 或域名：所要连接的VPN 服务器的信息

模式选择：选择加密模式，加密算法等。设置的模式与加密算法需要与对方一致。

3.7.2 VPN 的状态

显示VPN的连接状态，包括对方IP，本地子网，对方子网，状态，通讯包数量。

您当前的位置是：显示VPN连接状态

对方IP	本地子网	对方子网	状态	通讯包数量
192.168.10.254	192.168.1.0/255.255.255.0	192.168.0.0/255.255.255.0	已连接	1002817

3.7.3 PPTP 设置

用户可以设置PPTP的起始IP与终止IP，外网用户通过PPTP帐号拨进内网的时候，所获取到的IP地址段。

您当前的位置是： PPTP设置

设置

☐启用PPTP

起始IP

终止IP

确定

3.7.4 PPTP 用户

您当前的位置是：新增PPTP用户

PPTP用户设置

用户名 *

密　码 *

确认密码 *

固定IP

保存

1：固定IP是可选项,表示用此用户名登录则分配此IP,
注意IP地址需要在为PPTP分配的地址空间

- PPTP用户名：提供给外网拨入本VPN防火墙的PPTP用户的用户名。
- PPTP密码：提供给外网拨入本VPN防火墙的PPTP用户的密码。
- 固定IP：可以指定此PPTP用户所对应分配的IP，此IP必须在PPTP设置的IP范围内。

PPTP：点对点隧道协议

点对点隧道协议（PPTP）是一种支持多协议虚拟专用网络的网络技术。通过该协议，远程用户能够通过 Microsoft Windows NT 工作站、Windows 98，2000，XP，VISTA的操作系统以及其它装有点对点协议的系统安全访问公司网络，并能拨号连入本地 ISP，通过 Internet 安全链接到公司网络

3.8 流量管理

3.8.1 IP 流量控制

点击IP流量控制选项，可以输入一段IP地址进行上行和下行带宽的限制，输入完毕之后点击“保存”按钮保存生效。

显示IP速度列表

序号	起始IP	终止IP	上行带宽 (kbit/s)	下行带宽 (kbit/s)	UDP数	TCP数	WAN选择	启用
1			0	0			默认	☐
2			0	0			默认	☐
3			0	0			默认	☐
4			0	0			默认	☐

流量控制阀值： % (80-100) 启用流量控制阀值， WAN口流量要精确设置，则当总带宽超出阀值时，或过小时，会自动改变流量控制值，做到有效利用流量。

自动负载均衡： ☐ 上网每次连接自动选择出口线路，会根据剩余带宽选择出口， 如不设置外网带宽，则平均分配出口流量。

线路备份模式： ☐ WAN1作为主线路，其他线路不上线，WAN1掉线时，其他线路上线，WAN1重新上线时，其他线路会下线。

WAN1线路速度：(kbit/s) 上行带宽： 下行带宽：

WAN2线路速度：(kbit/s) 上行带宽： 下行带宽：

启动队列管理： ☐ (注意，启动队列管理将降低系统性能，如果需要使用保证最小带宽，则启动队列管理，精确设置WAN口带宽，配置带宽的上下行值,关闭队列管理要重启设备)

流量控制方式： 限制最大带宽 (没有启动队列管理，则只有限制最大带宽生效)

- 点击列出被控制的IP速度：点击后可以查看当前内网IP的外网上下行流量和WAN口的流量，可以按IP，速率来排列，能够有效的查看网络情况。
- 起始IP、终止IP：此为选择您所要限制的内网IP段或者单个IP。如果只限制单个IP，只需填入：192.168.1.100 to 100，则此规则就是针对192.168.1.100 此IP 做控制。若是要限制一组IP 范围，则填入如192.168.1.100 to 150，这样此规则就是针对192.168.1.100 到150 做限制。若是此条带宽限制是内网的所有IP 则可填入：192.168.1.0 to 0，这样就表示所有IP 都受此规则限制。
- 上行带宽：指对内网IP 的上传带宽。
- 下行带宽：指对内网IP 的下载带宽。

此处的速率为kbit/s，一般文件下载速率为KB/s，1KB=8Kbit。

- UDP数、TCP数：设置每台内网IP的UDP数和TCP数，建议分别设置为300。
- WAN选择：选择要设置的WAN口。

- 流量控制阀值：此阀值指的是所设置的WAN口带宽的阀值，当启用流量控制时，不设置或设为0表示始终启用流量控制， 否则表示当WAN口总使用率大于阀值时，流量控制才实际生效。在流量控制生效之后，系统无论流量是否达到阀值，都会执行流量控制5分钟，5分钟后，系统会再次侦测出此时的WAN口利用率，如果低于阀值则不启用流量控制，如果高于阀值，则再次启用流量控制。

注意：此功能只在最大带宽限制时使用，并需启用队列管理和设置WAN口带宽。

- 自动负载均衡：如果使用多条同一运营商的ADSL,可以选择自动负载均衡，则不需要在wan口配置中使用静态路由表，流量会自动使用多wan口传递数据，使数据均匀的从多WAN口传输。
- 线路备份模式：启用此功能后，WAN1则作为主线路，其他路线路不上线。当WAN1断开时，其他线路则上线。如果WAN1再次上线，其他线路又会再次下线。
- 启动队列管理：选择限制最小带宽时使用，启动队列管理将降低系统性能，如果需要使用保证最小带宽时，启动队列管理，精确设置WAN口带宽，配置最小带宽的上下行值,然后重启设备生效每台电脑的最大速度。
- WAN线路速度设置：参考3.4.2 WAN口配置
- 流量控制方式：

- 保障最小带宽： 如果此刻您采用的是10M光纤上网，您在外网带宽处设置下行带宽为8000kbit/s。当您下行的所有资源利用没有达到8000kb/s的时候，您的单个IP可以突破您所设置单个IP下行流量控制的数值，但是整个下行流量的总数值不会突破8000kb/s这个数值。当路由器整个下行流量的总数值达到8000kb/s，而且影响到了内网部分IP无法达到您所设置的单个IP下行流量数值的是时候，速率较高的IP的速率就会降低，能够保证内网的所有IP都能满足最小带宽。
- 限制最大带宽：为限制此条规则的最大可使用带宽，也就是最大不会超过此设定值。

3.8.2 会话列表



序号	类型	状态	源IP	源端口	目的IP	目的端口
1	tcp	CLOSE	192.168.0.10	2939	218.85.134.168	80
2	tcp	TIME_WAIT	192.168.0.10	2917	65.55.195.250	443
3	tcp	CLOSE	192.168.0.10	2903	218.16.227.85	80
4	tcp	TIME_WAIT	192.168.0.10	2920	121.14.117.146	80
5	tcp	CLOSE	192.168.0.10	2914	61.4.185.34	80
6	tcp	TIME_WAIT	192.168.0.10	2938	65.55.195.250	443
7	tcp	TIME_WAIT	192.168.0.10	2943	65.55.195.250	443
8	tcp	CLOSE	192.168.0.10	2942	218.85.134.168	80
9	tcp	CLOSE	192.168.0.10	2913	61.4.185.34	80
10	tcp	CLOSE	192.168.0.10	2930	218.85.134.168	80
11	tcp	CLOSE	192.168.0.10	2952	65.55.195.250	443
12	tcp	CLOSE	192.168.0.10	2933	218.85.134.168	80

本页显示当前的路由器的会话，您可以通过这个项目对当前所有的会话进行查看。会话按照“类型”“状态”“源IP”“源端口”“目的IP”“目的端口”来分类。您可以在查看处输入任何一个信息便可以查询到与此信息相关的所有会话。例如：如果您输入192.168.0.98，就会列出与此IP有关系的所有会话；如果您输入UDP，则只显示UDP的所有会话。

您还可以点击“列出按会话数最多的前10条”，可以查看当前会话数最多的10个IP的会话数。

按会话数降序排序的前10条

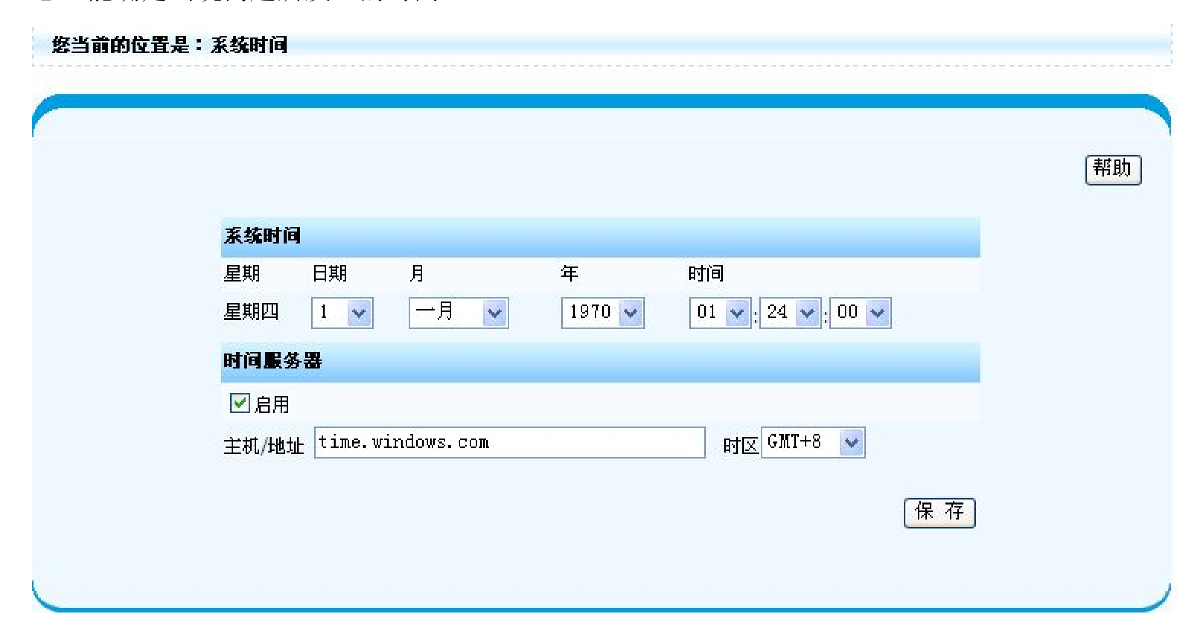
序号	源IP	会话数
1	192.168.0.98	51
2	192.168.0.10	16
3	192.168.0.11	8
4	59.172.72.142	3

刷新列表 确定

3.9 服务管理

3.9.1 时间设置

时间设置能将路由器的时间与用户所在时区的时间同步，方便用户管理路由器，查看系统日志，能确定出现问题所发生的时间。



- 系统时间：此处只能查看系统当前时间。
- 时间服务器：输入NTP服务器的主机名和地址。点击“保存”按钮同步本地和NTP服务器的时间，北京时间的时间服务器IP为：210.72.145.44。
- 启用：打开或关闭从时间服务器自动获取间的开关。

3.9.2 命令行工具



执行命令：在此输入您要执行的命令进行，可以执行的命令有 ping ， route ， free，ifconfig。

- ping ：此命令用于检测网络的连通。
- route ：此命令用于测试网络的路由功能和路由表。
- free：此命令用于显示内存的资源分配情况。
- ifconfig：此命令用于显示路由器的所有网络接口的连接信息和状态。

3.9.3 升级系统



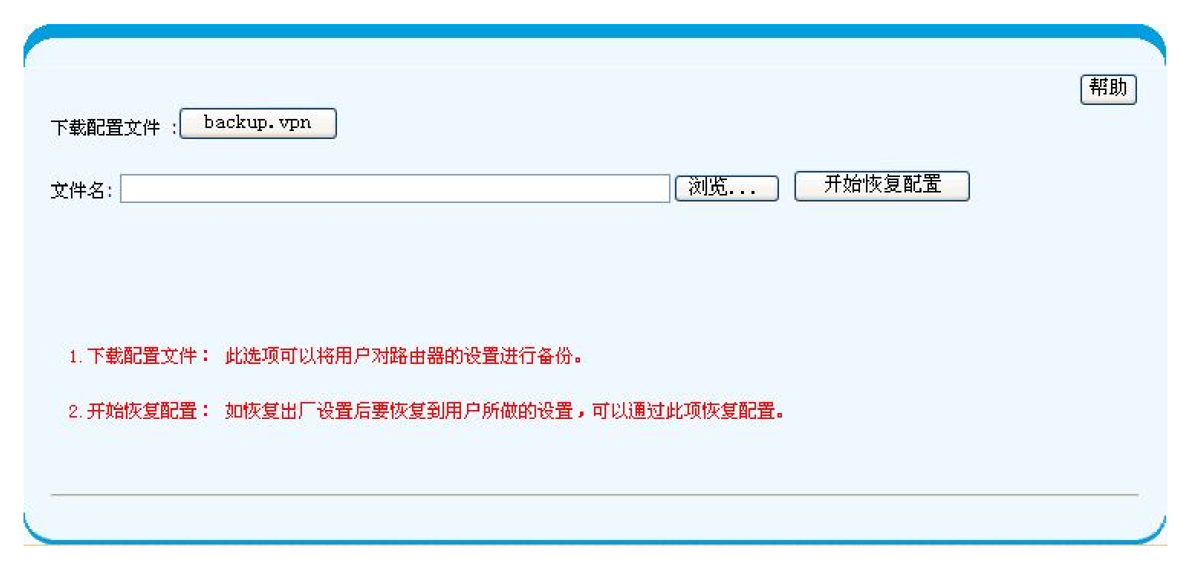
单击“浏览”按钮选择升级文件，然后单击“开始升级”按钮，文件将被上载到设备上，升级完成后，并重新启动。

注意:

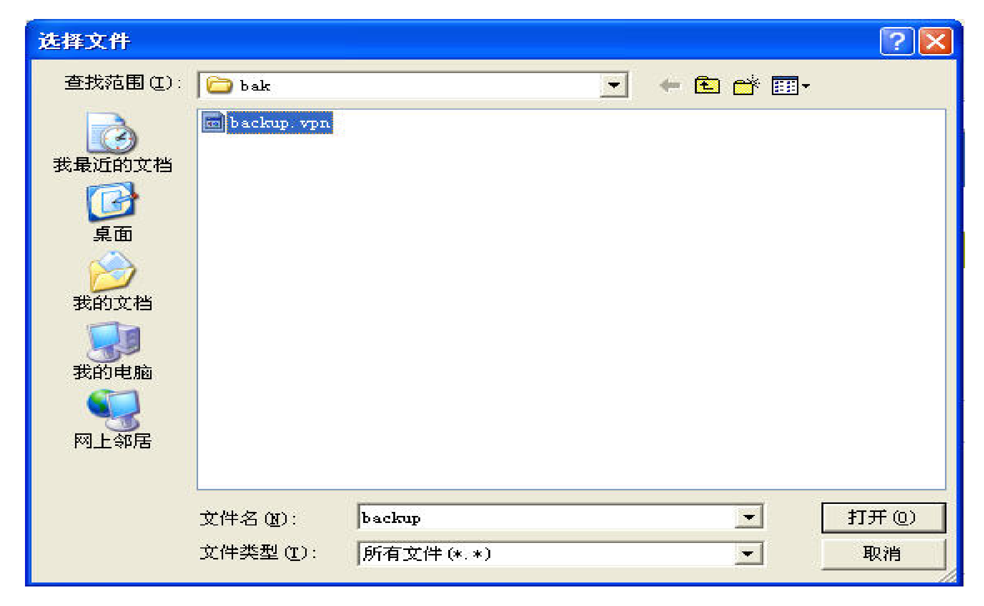
在升级过程中，请不要断电。升级完后介面将会自动出现“升级成功，请断电重新启动”。

3.9.4 配置备份与恢复

此选项可以将用户对路由器的设置进行备份。如恢复出厂设置后要恢复到用户所做的设置，可以通过此项恢复配置。



点击“backup.vpn”将路由器的配置文件保存到PC上，当需要恢复配置时点击“浏览”按钮，弹出如下界面：



然后选择保存到PC上的配置文件，点击“打开”按钮，点击“开始恢复配置”，当弹出“恢复配置成功”的界面即可。

🕮 注意:

备份的设置最好不要包含IP与MAC地址绑定设置，因为在另一个环境恢复了包含IP与MAC地址绑定设置的配置文件，很有可能会使路由器下连的PC无法与路由器相连。

3.9.5 恢复默认值



若是选择“确定”，会将所有的设定清除，并重新开机。我们建议在做版本升级前请先将Router现在的设定值存在计算机，等做完版本升级后，使用此功能将机器做出厂值设定以确保机器升级后的稳定行，然后再将刚才存在计算机的设定值存回(如何储存设定数据及升级完成后如何存回，请参考“配置备份与恢复”说明)。

3.10 用户认证

3.10.1 WEB 认证设置

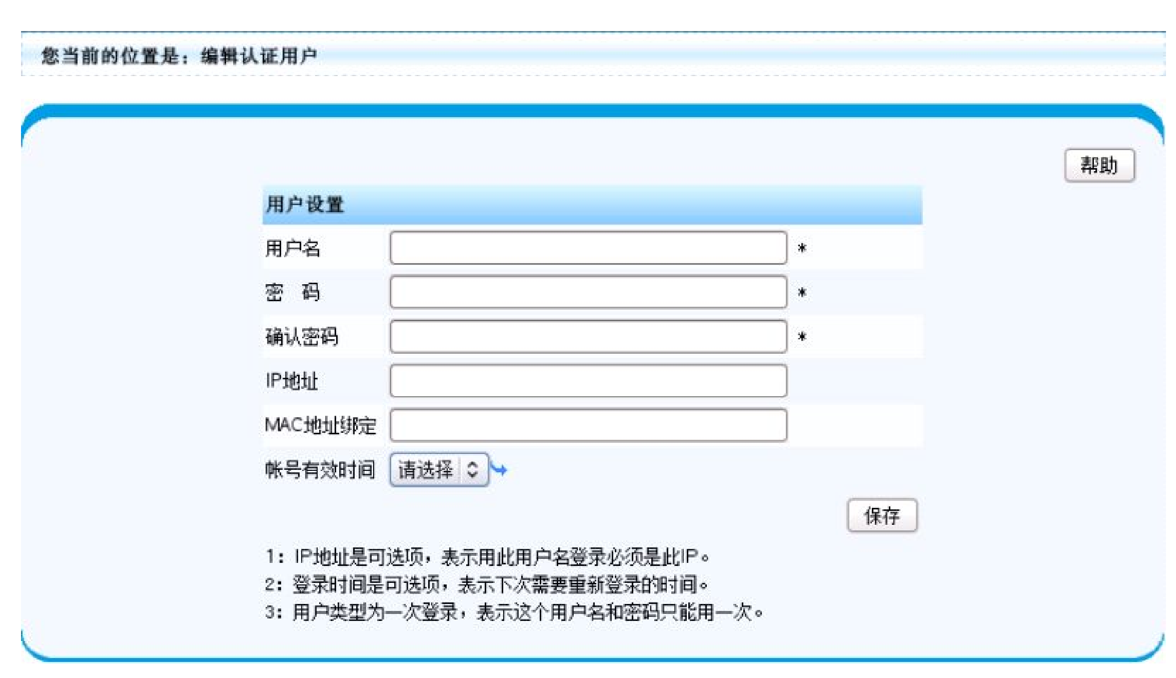


- 启用用户认证功能：选择后此功能方可生效。
- 退出时间：如果在后面用户设置中不设置认证时间，及以默认退出时间为准。
- 认证通过转向的网址：认证成功后，IE自动转向此网站，可以随意进行更改。
- 上传认证页面图片：上传认证图片后，在认证登陆界面时，会以此图片作为背景。

3.10.2 WEB 用户设置



- 可以通过“增加”添加一个新的认证用户。
- 页面内可以将设置的认证用户显示出来。



- “*”号为必填项目。
- 用户名：即为用户认证所输入的用户名。

- 密码：即为用户认证所输入的密码。
- 确认密码：确认输入过的密码。
- IP 地址：不填写则此用户名可以由任何内网用户来使用，填写则只由此 IP 的内网用户来使用。
- MAC 地址绑定：绑定固定的 MAC 地址,如果未非此 MAC 地址的用户则无法接入。
- 账号有效时间：可以设定有效时间，在此时间内，账户有效，超过则无效。

3.11 配置向导

此项可以帮助用户通过一步到位的方式配置一些简单的路由器信息，实现路由器能够正常上网。具体步骤如下：

- 第一步：向导使用说明
- 第二步：选择系统模式，当前设置只支持网关模式。
- 第三步：选择WAN口的接入方式，此设置向导只支持对WAN1口的设置向导，如需其他WAN口的设置，请到3.4.2中进行设置。
- 第四步：如选择ADSL拨号，填写用户名和密码。如其他方式，填写对应的信息。
- 第五步：选择性设置WAN口带宽
- 第六步：定义内网配置信息
- 第七步：DHCP服务器配置，配置是否打开DHCP服务器，以及DHCP分配的信息。
- 第八步：点击完成重启路由器，实现配置。

3.12 日志管理

3.12.1 日志配置



显示冗余日志：对于重复的系统日志信息进行显示。

打开告警日志：开启后会显示告警日志,显示告警信息提示用户出现病毒或者攻击。

激活 E-MAIL 功能：当日志达到最大值的一半适，系统会自动将日志信息以文本形式发送到所填写的 email 相关信息中，注意：此处尽可能的选择一些常用的 email 服务器。

每页显示记录条数：设置日志列表显示数目。

日志服务器地址：内网的日志服务器地址，可以在该 PC 上安装对应的日志服务器，日志信息可以直接保存于该 PC 的日志服务器上。

日志文件：可以将日志直接保存于附件用于查看分析。

3.12.2 系统日志

系统日志：提供了外部系统日志服务器收集系统信息功能。Syslog为一项工业标准通讯协议，网络上动态撷取有关的系统信息。系统日志提供了包含动作中的联机来源位置(Source IP Address)与目地(Destination IP Address)位置，服务编号(Port Number)以及型态(IP service)。输入您要查看的相关系统日志的服务器名称或是IP地址于“系统日志服务器”的空格字段内，您就可以查询到与此IP或者该信息相关的系统日志。



3.12.3 告警日志



告警日志：提示用户出现病毒或者攻击。

3.12.4 审计日志



审计日志：系统登录以及配置信息修改等行为的日志信息。

3.12.5 WEB 行为日志



WEB 行为日志：上网行为信息的日志，必须在防火墙策略控制中打开 web 行为日志。

3.12.6 IPSEC 日志



IPSEC 日志：将 VPN 中的 ipsec 相关信息通过日志形式体现出来。

3.13 修改帐号

当您每次登入至路由的设定画面时，必须输入密码。密码出厂值为“888888”。为了安全理由，我们建议您务必在第一次登入并完成设定之后更改管理密码！密码请牢记，若是密码忘记，将无法再登入至路由器的设定画面，必须回复到出厂值(Factory Default)。



- 修改登录密码：填写所更改密码。
- 确认登录密码：再填写一次更改密码。
- 修改：按下此按钮“修改”即会储存修改的密码。
- 密码最高只支持8位。

3.14 重新启动

您可以在此工具中选择系统重新启动，请按下“确定”按钮即可重新启动路由器。



3.15 退出

您点击退出后，可以安全退出WEB管理界面。

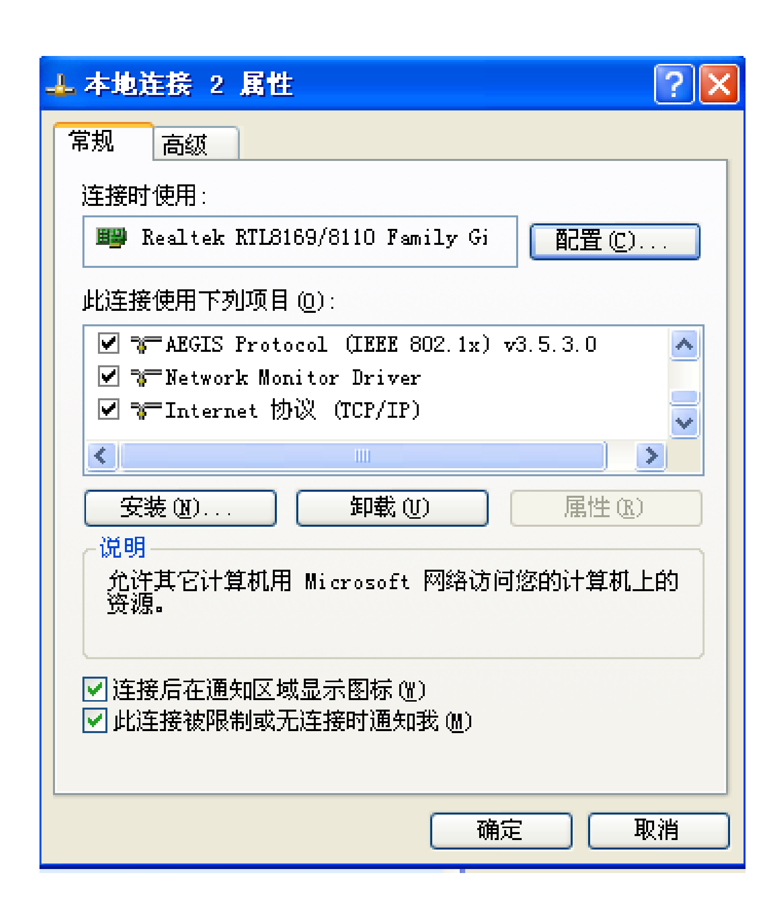
附录 A　FAQ

1 如何配置局域网中的计算机

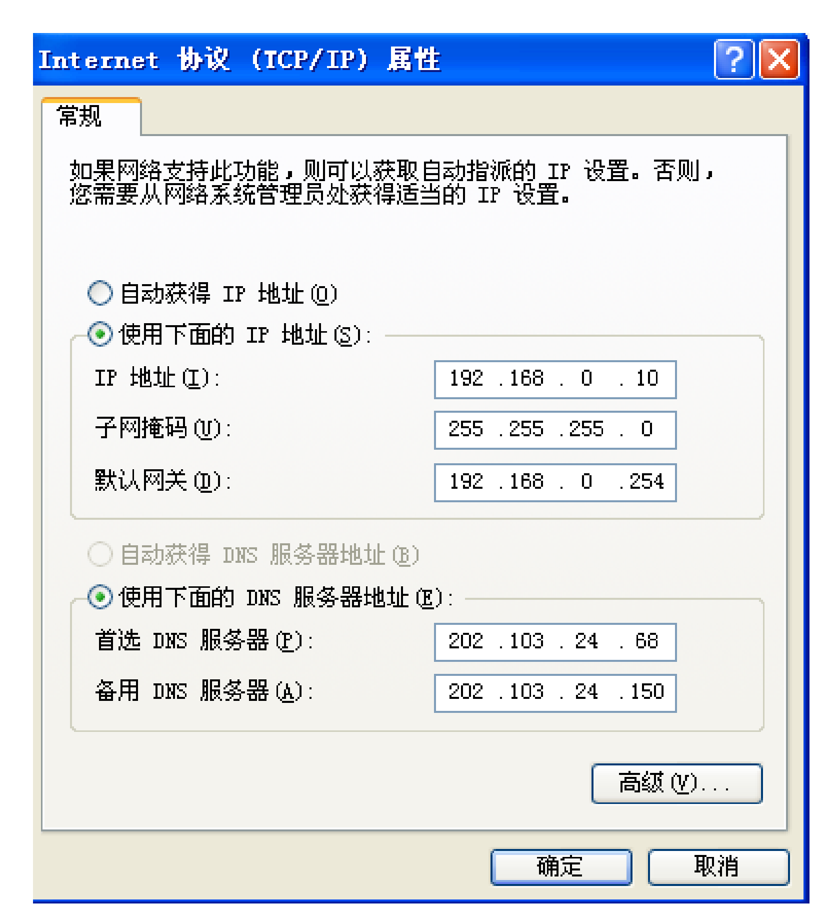
本章讲述如何在 Windows XP 环境下配置计算机的 TCP/IP 属性。下面分别介绍手工设置 IP 地址和通过 DHCP 服务器设置 IP 地址这两种情形下，配置 TCP/IP 属性的步骤。

一　手工设置 IP 地址

1. 单击“开始”→“设置” → “网络连接”，双击。
2. 双击“本地连接”图标，单击“属性”进入“常规”窗口。在“此连接使用下列项目”中，选择“internet 协议（TCP/IP）”选项；



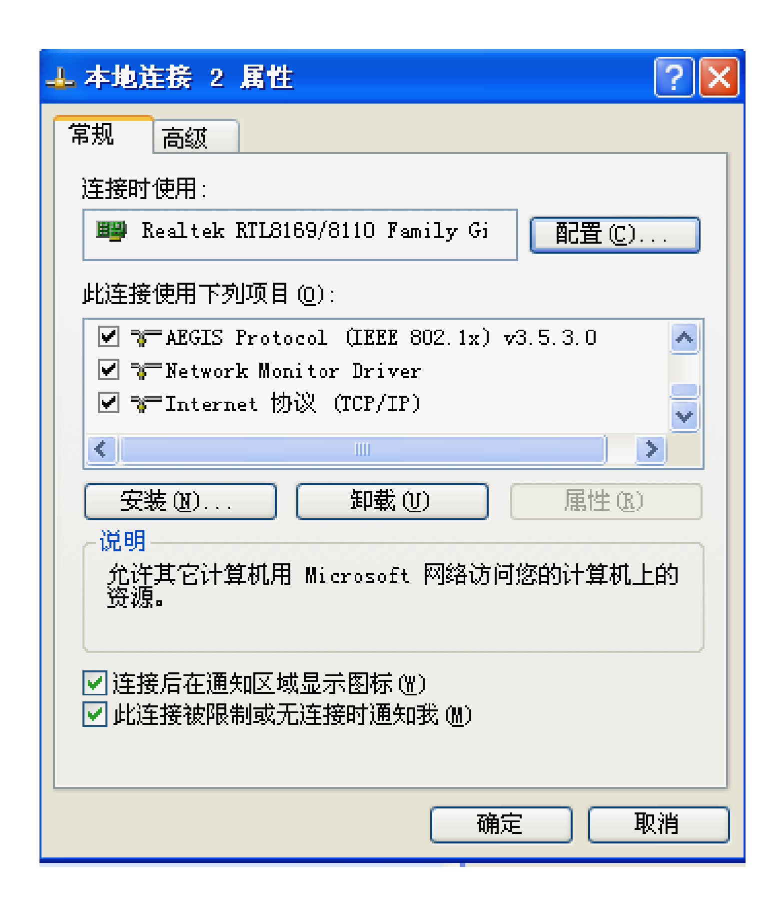
3. 首先选中“使用下面的 IP 地址”选项，然后在“IP 地址”中填入：192.168.0.X（X 在 2 至 253 之间），在“子网掩码”中填入 255.255.255.0，“默认网关”填入 VPN 防火墙的 IP：192.168.0.254；在“DNS 服务器”中填入当地 ISP 运营商提供的 DNS 服务器地址。



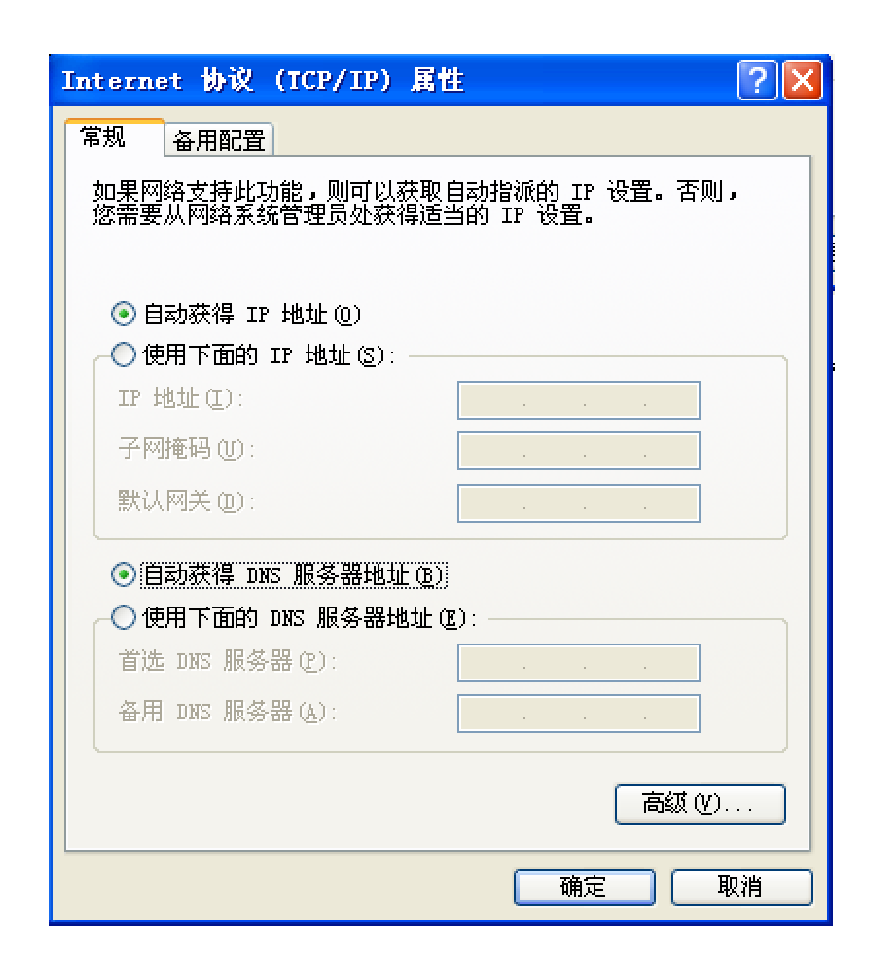
4. 以上配置完成后，单击“确定”按钮，配置 TCP/IP 属性完成。

方法二　通过 DHCP 服务器设置 IP 地址

1. 使用此功能之前，必须确保已经在 VPN 防火墙 的 DHCP 功能已开启（章节 3.5.1）；
2. 单击“开始”→“设置” → “网络连接”，双击。
3. 双击“本地连接”图标，单击“属性”进入“常规”窗口。在“此连接使用下列项目”中，选择“internet 协议（TCP/IP）”选项;



1. 首先选中“自动获得 IP 地址”和“自动获得 DNS 服务器地址”两个选项。

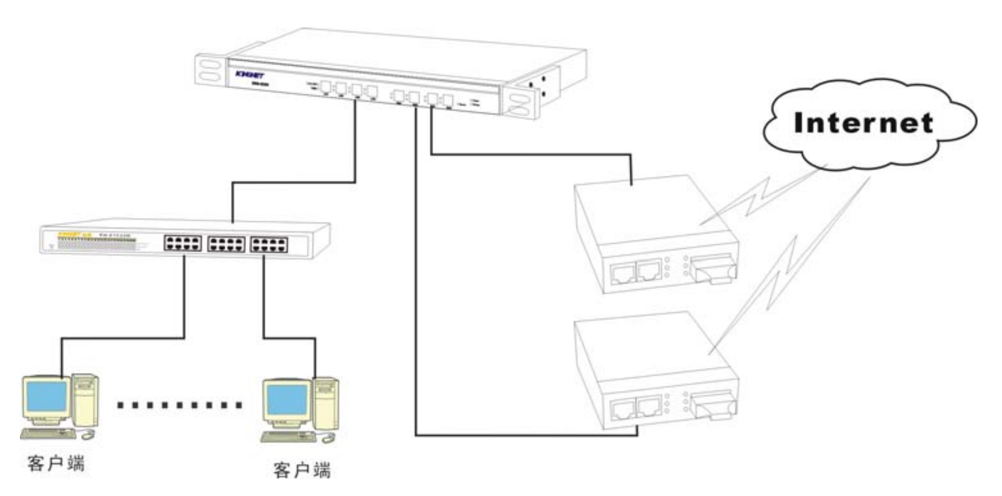


5. 以上配置完成后，单击“确定”按钮，配置 TCP/IP 属性完成。

2 如何实现多路 ADSL 上网

用户有时会采用多路 ADSL，这个时候，我们该如何对多路 ADSL 进行设置呢？应该注意哪些事项呢？下面我们对多路 ADSL 接入进行一个简单的介绍。

- 首先，将多路 ADSL 接入到 VPN 防火墙的 WAN 口，从 MODEM 接网线



- 然后进入 VPN 防火墙的 WEB 管理界面，对您所接入的 WAN 口进行配置：

填入 ISP 运营商给您提供的用户名和密码，多 WAN 口的 ADSL 设置相同，其他的设置按照默认设置。

WAN口配置方式

WAN口选择: WAN1　　配置方法: ADSL拨号连接

拨号连接配置选项

登录用户名	jxms5402	登录密码	●●●●●●●●●
从ISP得到DNS配置?	⦿ 是 ○ 否	特殊模式	○ 是 ⦿ 否
是否限制包尺寸?	1412 字节	是否进行LCP检测?	⦿ 是 ○ 否

WAN1 静态路由:

分行填写，格式如20.10.10.0/24

上行带宽:	450 kbit/s	下行带宽:	900 kbit/s
使用DNS查询检测断线:	☐	MAC地址克隆	00:10:22:45:14:26

连接已启动, IP = 58.48.63.96

保存

重　启

- 开启自动负载均衡（IP 流量控制中）

自动负载均衡: ☐　　上网每次连接自动选择出口线路，会根据剩余带宽选择出口，如不设置外网带宽，则平均分配出口流量

自动负载均衡开启，使得多路 ADSL 均衡使用调配，让网络资源更加有效的利用.

3 如何使用 DDNS 服务？

此处功能的设置在 网络配置→DNS 和 DDNS 配置 内。

所谓 DNS 是域名解析服务器的意思，即把域名转换成为网络可以识别的 IP 地址，使得互联网用户可以通过名称访问这个 IP 所指向的服务。对于通过 ADSL 上网的电脑而言，每次上网的时候有不同的 IP 地址，一般无法通过 DDNS 将域名固定指向这个固定的电脑。而 DDNS 服务（动态域名解析服务）就是把域名与这个动态的 IP 地址对应起来。

DDNS 的用途是什么？

简单而言，DDNS 可以将您的电脑变成一个互联网上的用户都可以访问的服务器，不过这个服务器是在您的家中或者单位里罢了。使用 DDNS 让您的电脑可用于：

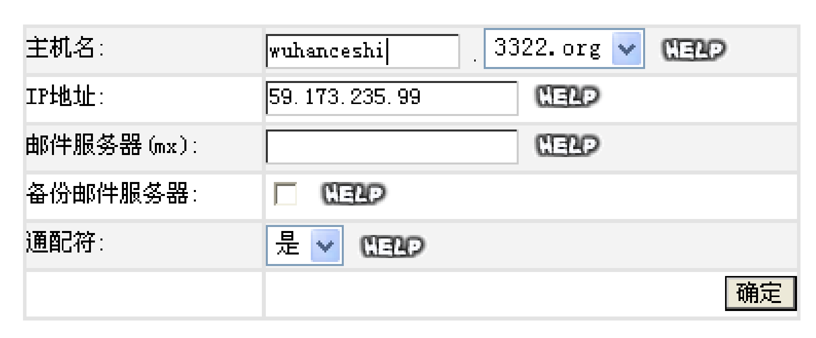
- Web 服务器——发布自己的网站并不受限制
- Mail 服务器——构建自己的邮件服务器收发邮件
- FTP 服务器——文件的上传或者下载
- VPN 服务器——不需要固定 IP 就可实现企业网之间的连接
- 远程访问服务器——随时随地管理自己的电脑

DDNS 如何实现？

需要一个能够提供 DDNS 服务的服务商，以便能够为您提供 DNS 解析服务。当您的 IP 发生变化的时候，能够立刻更改域名的指向，外网的用户都访问您新的 IP 所指向的电脑。其次，您的电脑上需要安装一个客户端软件，能够在您的电脑的 IP 地址发生变化的时候通过 DDNS 服务器进行新的解析服务。

VPN 防火墙的 DDNS 服务就是在 VPN 防火墙上内置了对应的客户端软件，使得用户在 VPN 防火墙内部不需要客户端软件就能享受 DDNS 服务。

1. 选择一个 DDNS 服务商，此处我们举例使用 3322 作为 dns 服务商
2. 登录 3322 服务商网站 vwww.3322.org，注册一个新的用户，然后登录。
3. 在管理域名中，添加一个新的动态域名，点击确定，如图所示：



4. 然后将此主机名和你所注册的 3322 用户名和密码填入到 VPN 防火墙的设置中去，点到“是”提交后，配置就完成了



5. 此时，你通过你所定义的主机名就能够访问到你现在的 VPN 防火墙，3322 会自动将你所填写的主机名解析到当前 VPN 防火墙的 WAN IP。



4 如何配置防火墙信息

此处功能的设置在 防火墙→设置选项 内。

防火墙的设置相对复杂，而且对于网络性能的影响也比较大，因此我们以网吧环境为参照提供部分参数的设置。对于网吧，必须要设置的内容：

防攻击 选项

选项	设置		已过滤
☑ 过滤 SYN 攻击	阀值:	包/每秒	已过滤 : 360 包
☐ 过滤 UDP 攻击	阀值:	包/每秒	已过滤 : 包
☑ 过滤 Ping of Death 攻击	阀值:	包/每秒	已过滤 : 包
☑ 过滤 Tear Drop 攻击			已过滤 : 包
☑ 过滤 IP Spoofing 攻击			已过滤 : 56160 包
☑ 常见攻击特征防范			已过滤 : 包
☐ 禁止本机被外网Ping			
☐ 禁止本机被外网访问			
☐ 限制非授权用户访问路由器(通过策略控制)			
☑ 限制用户每秒新建连接数	最大: 30	(10-40)	已过滤 : 22725 包
☐ 限制每个用户并发会话数	最大:	(100-400)	已过滤 : 包
☐ 打开告警日志			
☐ 启动UPNP功能			
日志服务器地址:			

- 过滤 SYN 攻击　　勾上即可，以默认值为限制
- 过滤 UDP 攻击　　一般网络情况不要采用，不然容易引起QQ、网络游戏不能正常使
- 过滤 Ping of Death　　一般设置为　200包/每秒
- 过滤 Tear Drop 攻击　　勾上
- 过滤 IP Spoofing 攻击　　勾上
- 常见攻击特征防范　　勾上
- 禁止本机被外网Ping　　勾上
- 禁止本机被外网访问　　需远程访问时不勾
- 限制非授权用户访问路由器(通过策略控制)　　需限制内网用户登录VPN防火墙勾上
- 限制用户每秒新建连接数　　一般设置为 30
- 限制每个用户并发会话数　　一般设置为 300
- 打开告警日志　　开启，在日志中将会出现告警
- 启动UPNP功能　　自动端口映射功能，根据客户自己需求选择
- 日志服务器地址　　内网作为日志服务器的PC所用的IP

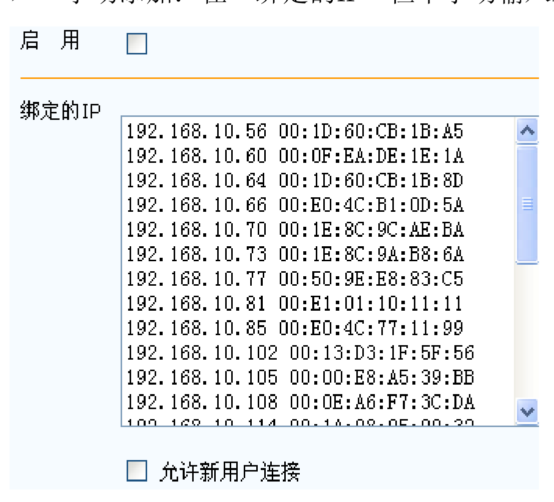
5 如何实现 IP+MAC 地址绑定

此处功能的设置在 网络配置→内网 IP 绑定 内。

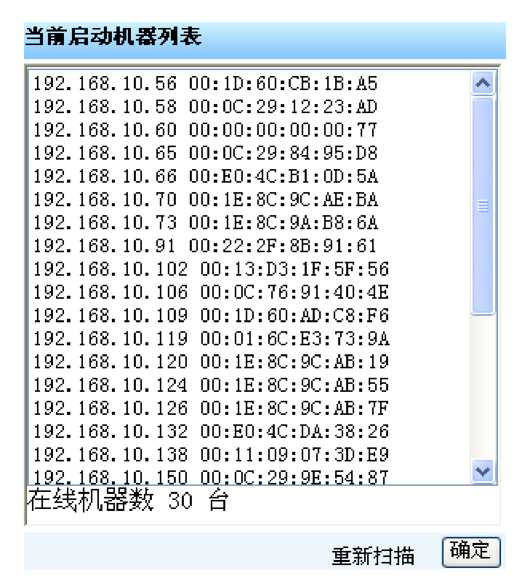
实现VPN防火墙下所带设备IP与MAC地址绑定的步骤：

1. 添加IP与MAC地址对应表（ARP列表）。对于VPN防火墙下所带设备的IP与MAC地址对应表我们可以手动添加，也可以通过VPN防火墙自动添加。

  - 手动添加：在“绑定的IP”栏中手动输入MAC与IP的对应列表。



  - 自动添加：点击“ARP列表”就可以显示出所有VPN防火墙下所带设备的IP与MAC地址对应表，复制这个列表到“绑定的IP”栏中。



2. 点击“内网IP绑定”中的“启用”按钮就可以把ARP列表中的IP与MAC实现一对一的绑定。
3. 允许新用户连接：当您不选择此项时，如果您在内网新接入一台PC，如果改PC没有进行IP+MAC绑定，那么它是无法上外网的；如果选择了此项，那么新接入的PC就可以上外网。

6 如何设置流量控制及智能流量控制

此处功能的设置在 流量管理→IP 流量控制 内。

由于网吧和企业的外网带宽是有限的，现在网吧国内提供的有10M，20M等多种，甚至个别为100M，企业可能用到的只是ADSL2M左右的带宽，但是这些带宽可以完全被下载软件所占用，从而严重影响到网络的速度。因此我们首先要将外网带宽的速度设置正确。如网络的上行带宽、下行带宽要填好。我们将介绍以最小带宽限制和最大带宽限制以及智能流量控制三种。

- 最小带宽限制方式

设置最小带宽的含义是保障内网用户的PC至少能够拥有您所设置的数值的流量。当系统的资源充足的时候，您的内网用户可以获取到更大的资源；当其他的用户所占用带宽低于您当前所设置的数值时，系统会自动降低其他用户的资源保障您的最小带宽，充分的发挥了资源利用率。一般情况下是与队列管理同时开启，此时，您还需要精确的设置您的WAN口带宽，从而实现资源拥有足够的冗余。

例如：您所使用的2M ADSL，您在WAN口带宽处设置为450K上行，1800K下行。然后在设置中

启用最小带宽管理模式，同时开启队列管理：

序号	起始IP	终止IP	上行带宽(kbit/s)	下行带宽(kbit/s)	启用
1	192.168.0.2	192.168.0.200	64	128	☑
2			0	0	☐
3			0	0	☐

流量控制阀值： %(0-100)　当启用流量控制时，不设置或设为0表示始终启用流量控制，否则表示当WAN口总使用率大于阀值时，流量控制才实际生效

自动负载均衡：☑　上网每次连接自动选择出口线路，会根据剩余带宽选择出口，如不设置外网带宽，则平均分配出口流量

线路备份模式：☐　WAN1作为主线路，其他线路不上线，WAN1掉线时，其他线路上线， WAN1重新上线时，其他线路会下线

启动队列管理：☑	(注意，启动队列管理将降低系统性能，如果需要使用保证最小带宽，则启动队列管理，精确设置WAN口带宽，配置带宽的上下行值,然后重启设备生效,关闭队列管理也要重启设备)	
WAN1线路速度:(kbit/s)	上行带宽: 450	下行带宽: 1800
WAN2线路速度:(kbit/s)	上行带宽:	下行带宽:
WAN3线路速度:(kbit/s)	上行带宽:	下行带宽:
WAN4线路速度:(kbit/s)	上行带宽:	下行带宽:
流量控制方式: 保障最小带宽	(没有启动队列管理，则只有限制最大带宽生效)	

- 最大带宽限制方式

设置最大带宽模式，即为您所设置的数字及即为内网PC所拥有的最大带宽，内网PC无法突破您所设置的数值，具体设置方式为：

序号	起始IP	终止IP	上行带宽(kbit/s)	下行带宽(kbit/s)	启用
1	192.168.0.2	192.168.0.200	200	800	☑
2			0	0	☐
3			0	0	☐

我们下面以网吧为例，例举出几种情况下应该如何设置最大带宽的数值：

带机量 / 带宽	100台	200台	300台
10M	<600K bit / s	<400K bit / s	<200K bit / s
20M	<700K bit / s	<500K bit / s	<400K bit / s
100M	<1000K bit / s	<800K bit / s	<600K bit / s

● 智能流量控制：

此方法是利用了系统所使用的流量控制阀值来智能的管理内网的用户，我们以一个实例来介绍此功能，一个外网接入为2M的ADSL网络，内网用户设置方式为下图：

序号	起始IP	终止IP	上行带宽(kbit/s)	下行带宽(kbit/s)	启用
1	192.168.0.2	192.168.0.200	100	400	☑
2			0	0	☐
3			0	0	☐

流量控制阀值：90 %(0-100)　当启用流量控制时，不设置或设为0表示始终启用流量控制，否则表示当WAN口总使用率大于阀值时，流量控制才实际生效

自动负载均衡：☑　上网每次连接自动选择出口线路，会根据剩余带宽选择出口，如不设置外网带宽，则平均分配出口流量

线路备份模式：☐　WAN1作为主线路，其他线路不上线，WAN1掉线时，其他线路上线，　WAN1重新上线时，其他线路会下线

启动队列管理：☑	(注意，启动队列管理将降低系统性能，如果需要使用保证最小带宽，则启动队列管理，精确设置WAN口带宽，配置带宽的上下行值,然后重启设备生效,关闭队列管理也要重启设备)	
WAN1线路速度:(kbit/s)	上行带宽: 450	下行带宽: 1800
WAN2线路速度:(kbit/s)	上行带宽:	下行带宽:
WAN3线路速度:(kbit/s)	上行带宽:	下行带宽:
WAN4线路速度:(kbit/s)	上行带宽:	下行带宽:
流量控制方式：限制最大带宽	(没有启动队列管理，则只有限制最大带宽生效)	

设置成为最大带宽流量限制模式，当内网的总流量没有达到WAN口线路速度的90%的时候，系统将不启用流量控制功能，此功能不生效，内网用户可以享用超过最大带宽设置的流量。但是，当内网的总流量达到了WAN口总带宽的90%的时候，系统将自动启动最大带宽管理，将内网的每台PC速度限制在上行100kbit/s,下行400kbit/s以下。

在系统执行此命令5分钟后，系统将重新识别当前的内网总流量是否达到WAN口带宽的90%,如果没有达到，那么最大带宽限制将再次失效，用户能享用更充足的网络资源，此时，如果总流量再次达到WAN口带宽的90%，那么此时最大带宽限制流量控制将再次生效。周而复始，让内网流量控制更加智能的启用，让内网用户更方便快捷的上网。

7 如何实现对内网用户上网权限的设置

此处功能的设置在 防火墙→数据报控制策略 内。

对内网用户上网权限的设置可以灵活使用，您只需要参考前面说明书对各项的定义，然后参考我们下面为您举的例子，您便可以轻松灵活的使用此功能。例如：

如果有一家公司，用户权限分为经理，普通员工，网管。

网管的权限是可以登录VPN防火墙进行管理，能够上外网。

经理的权限是无法登录VPN防火墙进行管理，能够上外网。

普通员工的权限是无法登录VPN防火墙进行管理，不能上QQ和网页，其他一些网络服务能使用。

➢ 第一步：因为此处涉及到对VPN防火墙的管理，所以必须在防火墙设置选项中将“限制非授权用户访问路由器(通过策略控制)”打钩。

☑ 限制非授权用户访问路由器(通过策略控制)

➢ 第二步：在IP管理中定义网管，经理，普通员工3个不同的IP组，以及VPN防火墙管理IP。

您当前的位置是： IP设置

序号	名称	IP地址	子网掩码	MAC地址	操作
1	网管	192.168.0.1	255.255.255.255		修改 删除
2	总经理	192.168.0.2-192.168.0.4			修改 删除
3	普通员工	192.168.0.5-192.168.0.20			修改 删除
4	路由管理IP	192.168.0.254	255.255.255.255		修改 删除

➢ 第三步：实现经理及普通员工无法登录VPN防火墙进行管理，普通员工不能上QQ和网页。定义4条访问规则，分别定义经理和普通员工无法访问VPN防火墙IP，普通员工封锁QQ，普通员工封锁80端口。规则编辑如下（没指明的不更改）：

序列号：001

内容过滤：选择到数据包

方向：内网到外网

内网IP：选择经理

外网IP：选择VPN防火墙管理IP

IP类型：ALL

当以上条件符合时：拒绝

序列号：002

内容过滤：选择到数据包

方向：内网到外网

内网IP：选择普通员工

外网IP：选择VPN防火墙管理IP

IP类型：ALL

当以上条件符合时：拒绝

序列号：003

内容过滤：选择到封锁QQ

方向：内网到外网

内网IP：选择普通员工

IP类型：ALL

当以上条件符合时：拒绝

序列号：004

内容过滤：选择到数据包

方向：内网到外网

内网IP：选择普通员工

服务：选择到80端口对应的HTTP

IP类型：ALL

当以上条件符合时：拒绝

您当前的位置是：访问规则

序列号	内网IP	外网IP	服务	方向	IP类型	策略	状态	操作
001	总经理	路由管理IP		内网->外网	all	拒绝	打开	修改 删除
002	普通员工	路由管理IP		内网->外网	all	拒绝	打开	修改 删除
003	普通员工			内网->外网	all	拒绝	打开	修改 删除
004	普通员工		HTTP	内网->外网	all	拒绝	打开	修改 删除

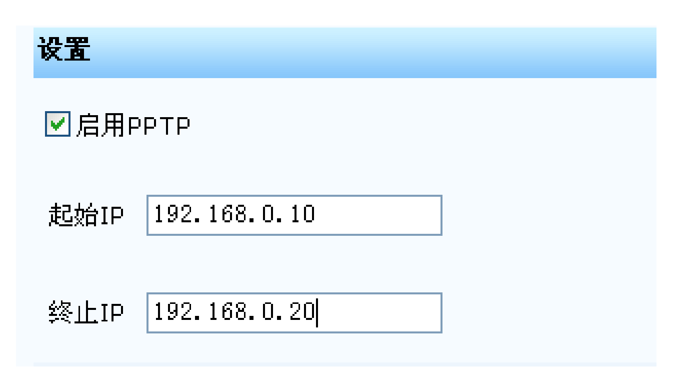
定义以上4条规则后，就能满足上文中所提出的需求。

8 如何通过 PPTP 建立 VPN 连接

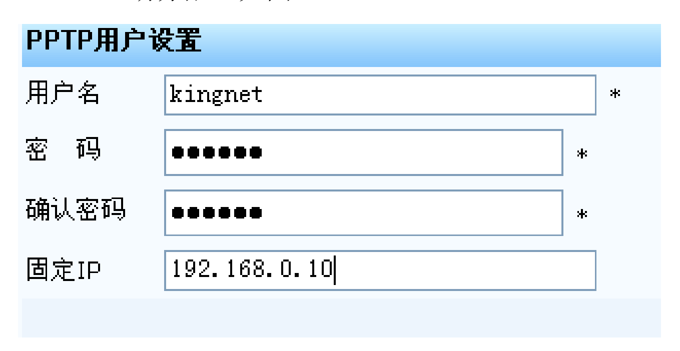
此处功能的设置在 VPN 配置 内：

PPTP 连接即为外网用户通过 PPTP 拨号，接入到您的设备中来，从而建立起 VPN 连接，下面我们对如何进行此项配置进行详细说明。

- 首先，您需要在您的 VPN 防火墙上启用 PPTP 用户，开启一个 IP 段作为外网用户的接入，如图 ：



- 然后，设置 PPTP 用户登录信息，您可以指定该帐号接入后获取 IP 为指定 IP,也可以自动分配，如图：

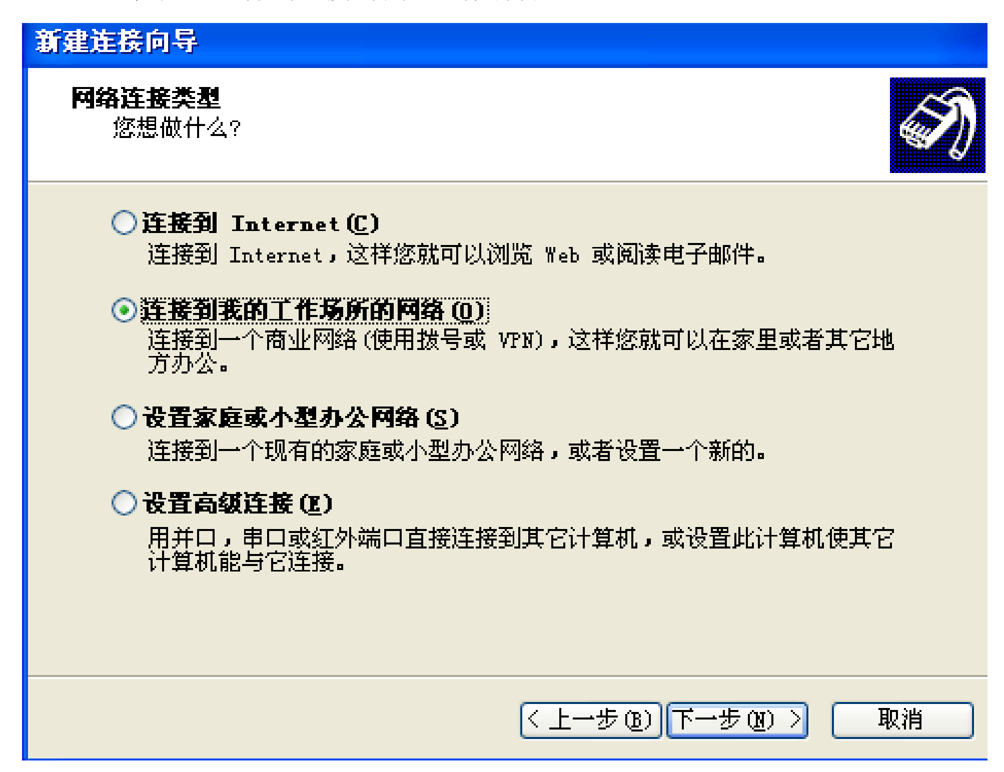


在对 VPN 防火墙上进行好设置之后，我们例举在 WINDOWS XP 下建立 PPTP 连接：

- 首先，在 WINDOWS XP 系统下打开网络连接，点击左侧的网络任务：创建一个新的连接



- 然后，选择到连接到我的工作场所的网络



- 再选择到虚拟专用网络连接：

新建连接向导

网络连接
您想要在工作点如何与网络连接?



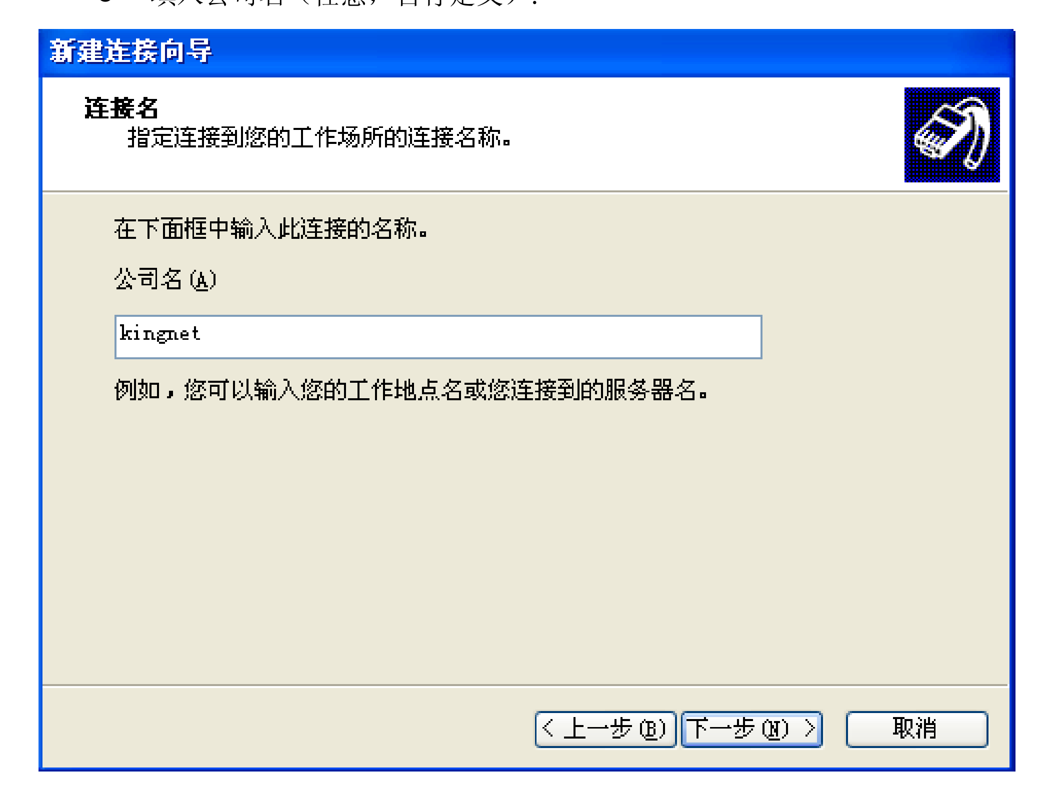
创建下列连接:

拨号连接 (D)
用调制解调器和普通电话线连接，或通过综合业务数字网 (ISDN) 电话线连接。

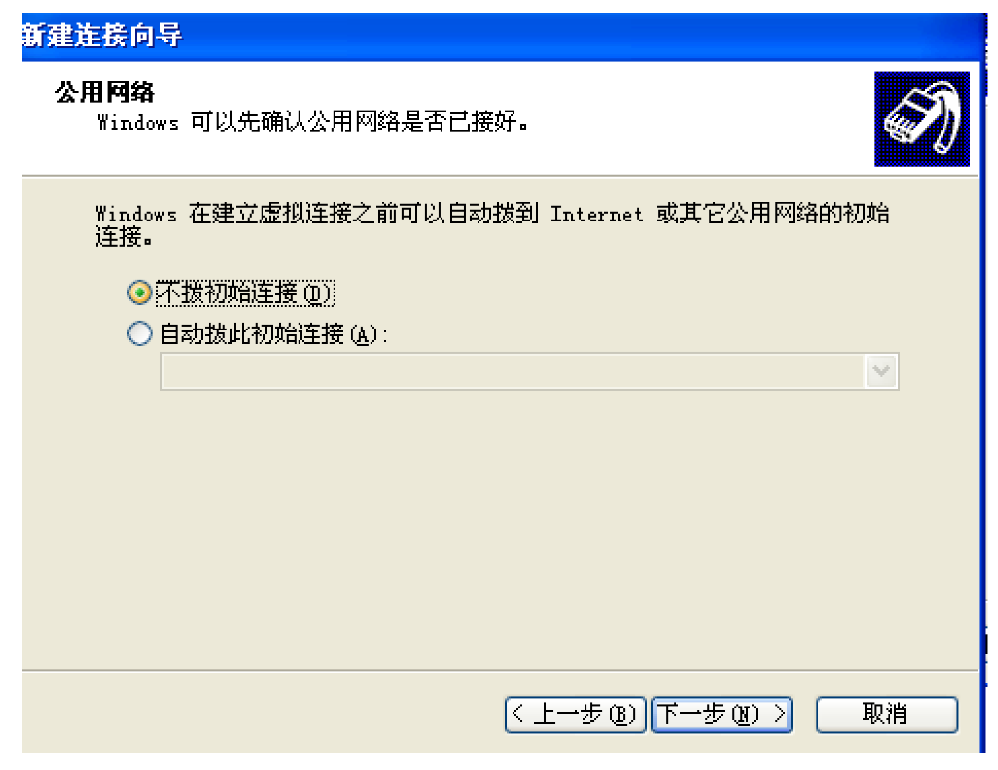
虚拟专用网络连接 (V)
使用虚拟专用网络 (VPN)通过 Internet 连接到网络。

< 上一步 (B)　下一步 (N) >　取消

● 填入公司名（任意，自行定义）：



● 选择不拨初始连接：



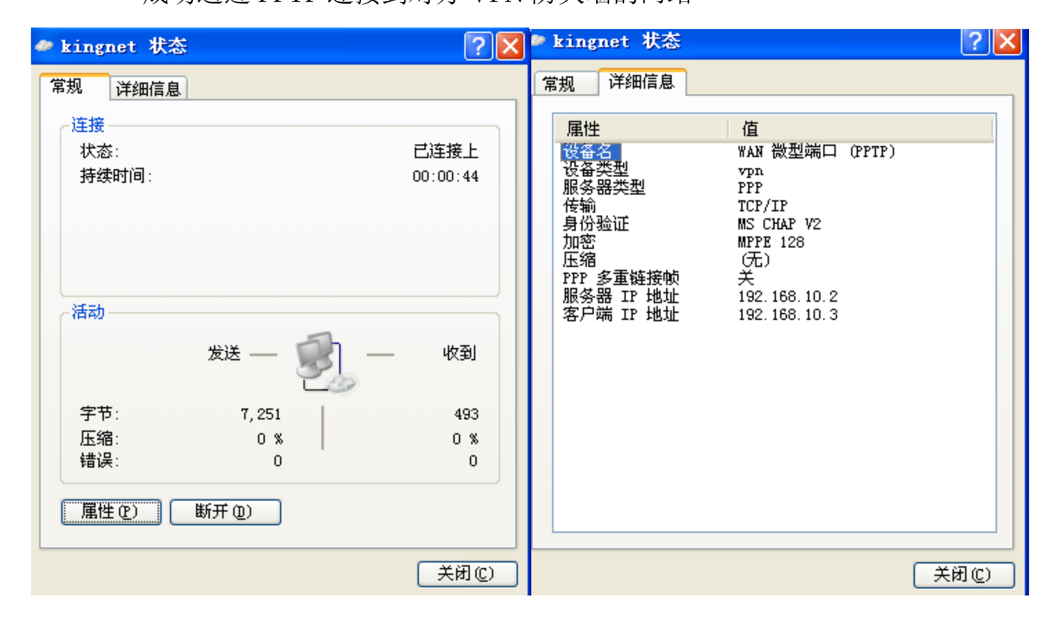
- 填入您所需要拨入的 VPN 防火墙的 WAN 口 ip：



- 完成输入后，在此处输入之前在 VPN 防火墙定义的帐号和密码进行拨号:



● 成功通过 PPTP 连接到对方 VPN 防火墙的网络



● 您可以直接通过 ping 命令来检测是否于对方局域网连通：

```
Pinging 192.168.10.1 with 32 bytes of data:

Reply from 192.168.10.1: bytes=32 time=144ms TTL=64
Reply from 192.168.10.1: bytes=32 time=212ms TTL=64
Reply from 192.168.10.1: bytes=32 time=134ms TTL=64
Reply from 192.168.10.1: bytes=32 time=222ms TTL=64
Reply from 192.168.10.1: bytes=32 time=129ms TTL=64
```

9 如何实现 2 台 VPN 防火墙的 VPN 连接

如果让两台 VPN 防火墙如何实现 VPN 连接，首先我们对 VPN 的概念进行一个初步的认识

📖 说明

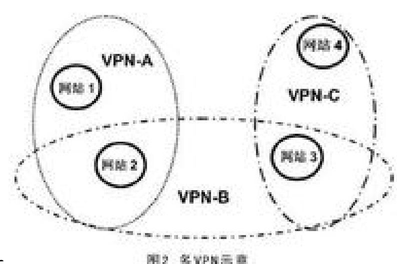


图2 多VPN示意

VPN的英文全称是“Virtual Private Network”，翻译过来就是“虚拟专用网络”。顾名思义，虚拟专用网络我们可以把它理解成是虚拟出来的企业内部专线。它可以通过特殊的加密的通讯协议在连接在Internet上的位于不同地方的两个或多个企业内部网之间建立一条专有的通讯线路，就好比是架设了一条专线一样，但是它并不需要真正的去铺设光缆之类的物理线路。这就好比去电信局申请专线，但是不用给铺设线路的费用，也不用购买路由器等硬件设备。VPN技术原是路由器具有的重要技术之一，目前在交换机，防火墙设备或WINDOWS2000等软件里也都支持VPN功能，一句话，VPN的核心就是在利用公共网络建立虚拟私有网。

建立2台VPN防火墙的VPN连接，首先要在其中一台VPN防火墙上建议VPN连接的服务端。服务端，顾名思义，是作为这个连接的服务器端，供另外一端接入。在另外一台VPN防火墙建一个客户端，用于接入到这台VPN防火墙的服务端中去，从而实现了两台VPN防火墙的VPN连接。下面，我们对VPN防火墙的VPN设置进行一个说明:

- 首先要确定的两台VPN防火墙的内网IP必须是不同的，这样不会造成VPN连接出现错误

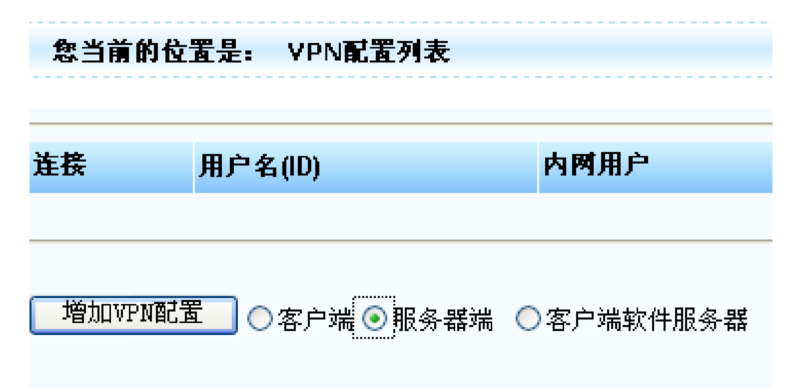
VPN防火墙一，假设为总公司

接口名称	IP地址
内网（编辑）	192.168.10.1

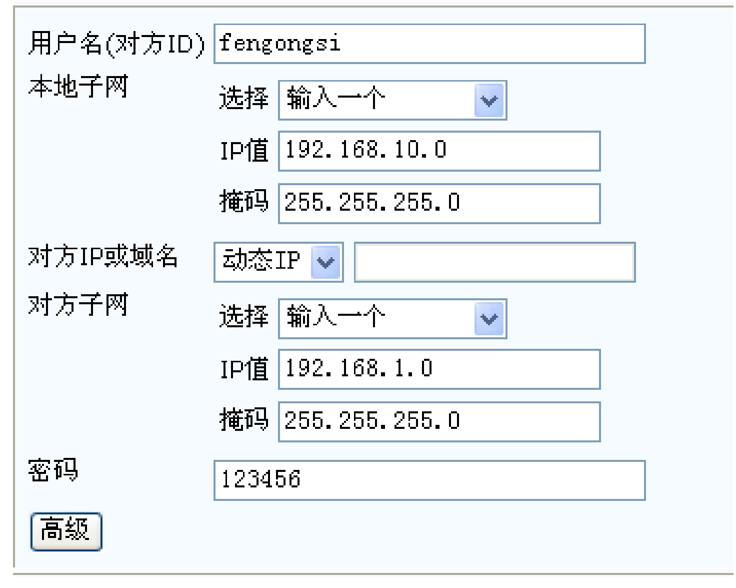
VPN防火墙二，假设为分公司

接口名称	IP地址
内网（编辑）	192.168.1.1

- 其次，将VPN防火墙一（总公司）作为VPN连接的服务端

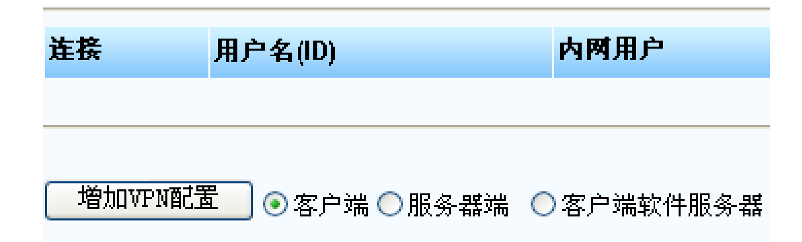


在此处填入供客户端接入的用户名，以及服务端的本地子网以及接入的客户端的本地子网，以及供对方接入的IP或域名，此处选择为动态IP即可，且需设置供客户端接入的密码。

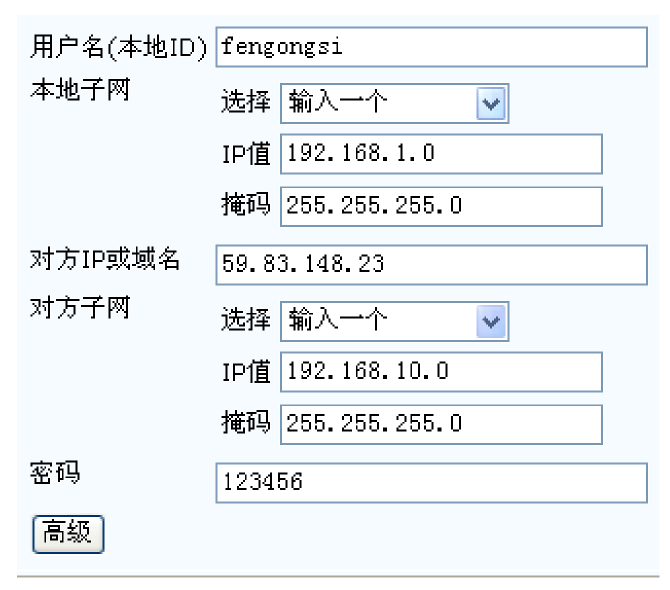


保存后并让设置生效

- 将VPN防火墙二（分公司）作为VPN连接的客户端



在此处填入客户端接入的用户名，要与服务端提供的用户ID相匹配；以及服务端的本地子网以及接入的客户端的本地子网，以及服务端的WAN口 IP或者域名，且需设置服务端提供的密码。



保存后并让设置生效

- 可以在VPN状态中查询到当前的连接状态

您当前的位置是：显示VPN连接状态

对方IP	本地子网	对方子网	状态	通讯包数量

10 如何设置静态路由

下面就以几个典型应用为例，来说明一下什么情况需要设置静态路由，静态路由条目的组成，以及静态路由的具体作用。

例一：最简单的串连式双路由器型环境

这种情况多出现于中小企业在原有的路由器共享Internet的网络中，由于扩展的需要，再接入

一台路由器以便连接另一个新加入的网段。而家庭中也很可能出现这种情况，如用一台宽带路由器共享宽带后，又加入了一台无线路由器满足无线客户端的接入。

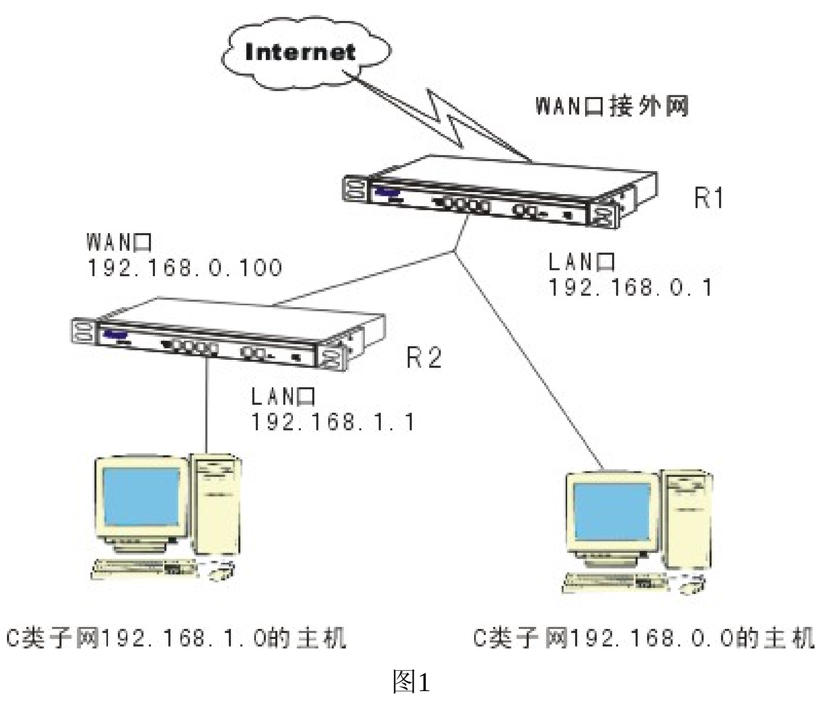


图1

（注：图中省略了可能存在的交换层设备）

如图1所示，LAN 1为192.168.0.0这个标准C类网段，路由器R1为原有路由器，它的WAN口接入宽带，LAN口（IP为192.168.0.1）挂着192.168.0.0网段（子网掩码255.255.255.0的C类网）主机和路由器R2（新添加）的WAN口（IP为192.168.0.100）。R2的LAN口（IP为192.168.1.1）下挂着新加入的LAN 2这个192.168.1.0的C类不同网段的主机。

如果按照共享Internet的方式简单设置，此时应将192.168.0.0的主机网关都指向R1的LAN口（192.168.0.1），192.168.1.0网段的主机网关指向R2的LAN口（192.168.1.1），那么只要R2的WAN口网关指向192.168.0.1，192.168.1.0的主机就都能访问192.168.0.0网段的主机并能通过宽带连接上网。这是因为前面所说的宽带路由器中一条默认路由在起作用，它将所有非本网段的目的IP包都发到WAN口的网关（即路由器R1），再由R1来决定信息包应该转发到它自己连的内网还是发到外网去。但是192.168.0.0网段的主机网关肯定要指向192.168.0.1，而R1这时并不知道192.168.1.0这个LAN 2的正确位置，那么此时只能上网以及本网段内的互访，不能访问到192.168.1.0网段的主机。这时就需要在R1上指定一条静态路由，使目的IP为192.168.1.0网段的信息包能转发到路由器R2去。

一条静态路由条目一般由3部分组成：1.目的IP地址或者叫信宿网络、子网；2.子网掩码；3.网关或叫下一跳。

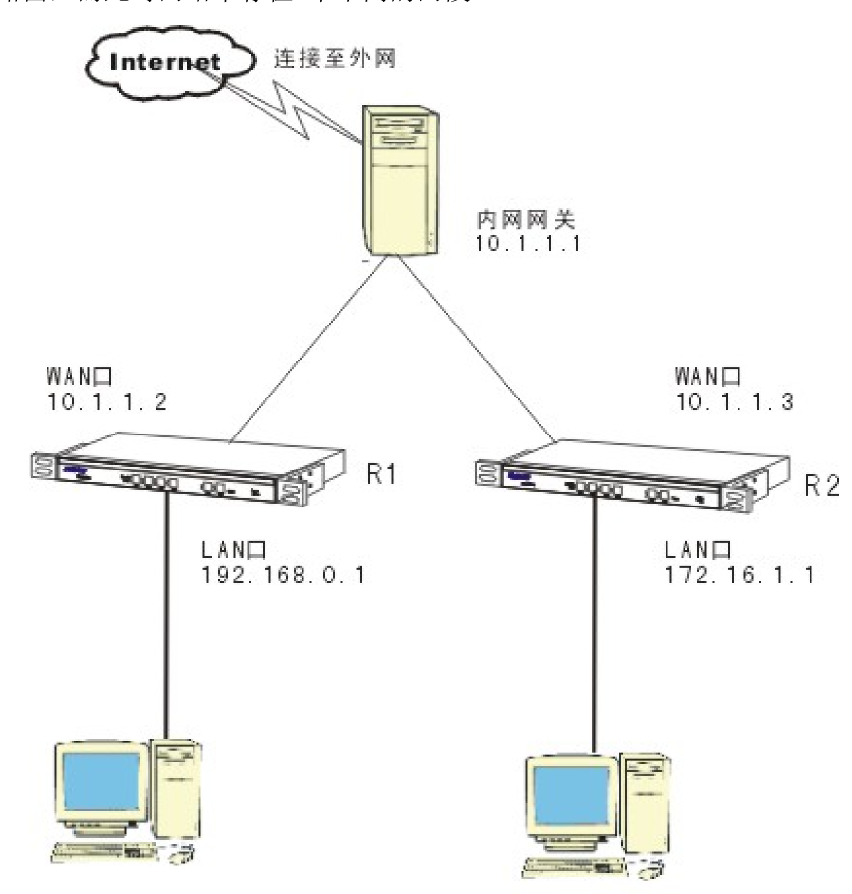
例1中R1上设定的静态路由条目就应该为：目的IP地址192.168.1.0（代表1.x这个网段），子网

掩码255.255.255.0（因为是C类网段），下一跳192.168.0.100。如图2，此图为TP-LINK R410中的静态路由表配置项，保存后即可生效。

注意：其中的网关IP必须是与WAN或LAN口属于同一个网段。那条默认路由写出来就是：目的IP为 0.0.0.0，子网掩码0.0.0.0，下一跳为WAN口上的默认网关，有时我们也称它为“8个0的默认路由”。另外，如果目的IP是一个具体的主机IP（如192.168.1.2），那么路由条目应为：目的IP 192.168.1.2，子网掩码255.255.255.255，下一跳或网关192.168.0.100。

例二：两台平级并连的路由器，下挂子网中主机需要互相通信的环境

这种情况，两台平行并连的路由器上层应该还有一个总的出口网关，而这个网关有可能因某种原因不便设置路由，而此时网络中存在3个不同的网段。



图中内网网关就是小区的网关，R1和R3分别为两户的宽带路由器，它们之间一般通过楼层的接入交换机和小区的骨干交换机连接在一起，此图省略了这一部分。图4的这种情况，只要在网关设备上按例一的方式添加两条路由就能实现两个子网中主机的互访，而且其10.0.0.0这个A类网段中存在的主机也都能通过这两条路由访问到R1和R3下的内网机。但是如果是小区的网关设备，那

肯定是不会让用户随便配置路由条目的，而且你应该也不想小区内的所有用户都能直接访问到你的内网主机。这时，我们可以在R1和R3上各添加一条路由指向对方来实现R1和R3下主机直接互访的效果。

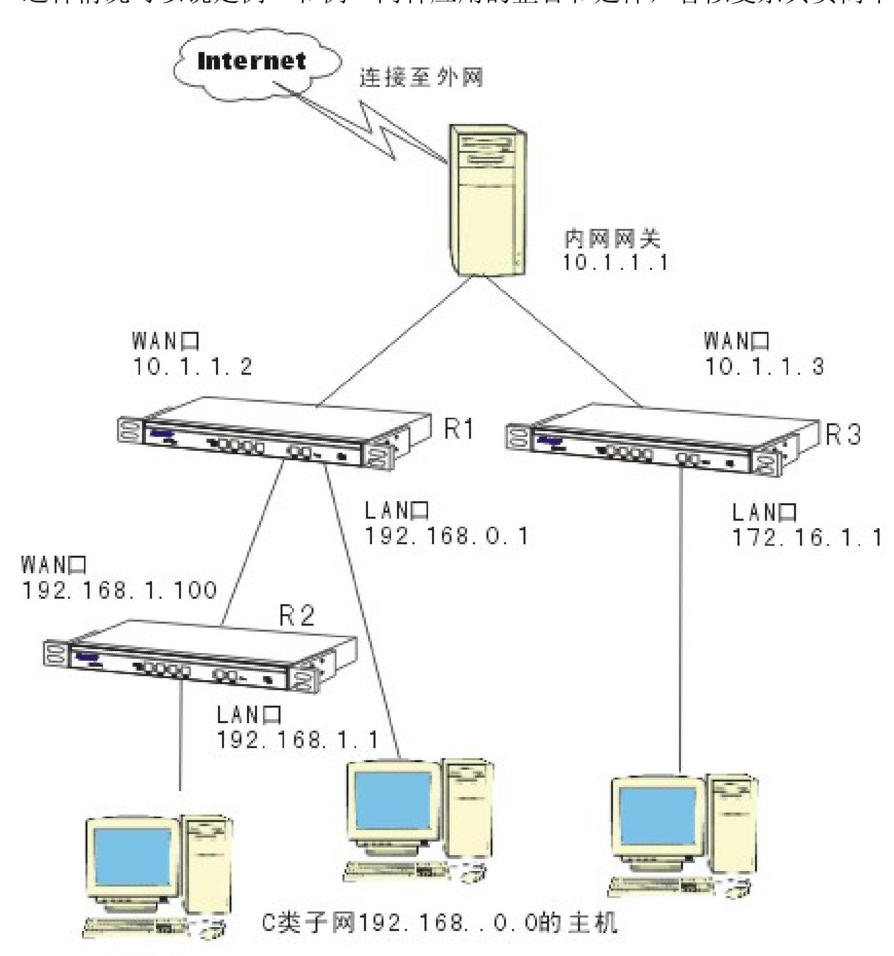
在R1上：目的IP地址172.16.0.0，子网掩码255.255.0.0（B类网段），下一跳10.1.1.3

在R3上：目的IP地址192.168.0.0，子网掩码255.255.255.0（C类网段），下一跳10.1.1.2

注：有些新型小区中使用了P-VLAN技术，这种网络的情况比较复杂，这样上面简单的静态路由设置有可能无法达到目的。

例三：既串且并，网络中有多级路由设备的环境。

这种情况可以说是例一和例二两种应用的整合和延伸，看似复杂其实简单



C类子网192.168.1.0的主机　　　　B类子网172.16.0.0的主机

既然拓扑图是例一、例二的结合，那将例一、例二中的路由条目加在一起是不是就可以了呢？当然也不是这么简单，如果只是配置了前两例的路由条目，R3下的主机是无法直接访问到R2下的192.168.1.0这个子网的。所以在R3上还要加一条到192.168.1.0这个子网的路由。静态路由条目配置如下：

R1：目的IP地址192.168.1.0，子网掩码255.255.255.0，下一跳192.168.0.100。

目的IP地址172.16.0.0，子网掩码255.255.0.0，下一跳10.1.1.3。

R3：目的IP地址192.168.0.0，子网掩码255.255.255.0，下一跳10.1.1.2。

目的IP地址192.168.1.0，子网掩码255.255.255.0，下一跳10.1.1.2。

如例三中，R3上的第一条：目的IP为192.168.0.0；第二条：目的IP为192.168.1.0。我们只提取了前面的两段192.168，而后面的第三段网络位中还是有相同的部分的。192.168.0.0中第三段写成二进制数为00000000（8位0），182.168.1.0中第三段写成二进制数为00000001（7位0，1位1），那么它们的前7位是相同的，在对应的子网掩码位置上就应该是11111110（7位1，1位0），合成十进制为254。所以这条汇总路由应该写成：目的IP为192.168.0.0，子网掩码255.255.254.0，下一跳10.1.1.2。这样，这条汇总路由只包含192.168.0.0和192.168.1.0两个子网，是一条精确的汇总路由。如图6中，R3下172.16.0.0的主机发送到192.168.2.0网段的信息包，其第三段网络位写成二进制为00000010（前6位0），就不包含在这条精确的汇总路由内了。

这时我们在R3上静态路由条目应该为

1.目的IP地址192.168.0.0，子网掩码255.255.254.0，下一跳10.1.1.2。

2.目的IP地址192.168.2.0，子网掩码255.255.255.0，下一跳10.1.1.4。

附录 B　分位表示法对照表

分位表示法	子网掩码
1	128.0.0.0
2	192.0.0.0
3	224.0.0.0
4	240.0.0.0
5	248.0.0.0
6	252.0.0.0
7	254.0.0.0
8	255.0.0.0
9	255.128.0.0
10	255.192.0.0
11	255.224.0.0
12	255.240.0.0
13	255.248.0.0
14	255.252.0.0
15	255.254.0.0
16	255.255.0.0
17	255.255.128.0
18	255.255.192.0
19	255.255.224.0
20	255.255.240.0
21	255.255.248.0
22	255.255.252.0
23	255.255.254.0
24	255.255.255.0
25	255.255.255.128
26	255.255.255.192

27	255.255.255.224
28	255.255.255.240
29	255.255.255.248
30	255.255.255.252
31	255.255.255.254
32	255.255.255.255